U.S. Department of Transportation

United States Coast Guard

MILITARY PERSONNEL SECURITY PROGRAM

COMDTINST M5520.12B

U.S. Department of Transportation
United States Coast Guard

Commandant
United States Coast Guard

2100 2nd ST SW
Washington, DC 20593-0001
Staff Symbol: G-CFI
Phone: (202) 267-1481

COMDTINST M5520.12B
SEP 4 2001

COMMANDANT INSTRUCTION M5520.12B

Subj: MILITARY PERSONNEL SECURITY PROGRAM

1. PURPOSE. To provide military personnel security policies, standards and procedures.

2. ACTION. Area and district commanders, commanders of maintenance and logistics commands, commanding officers of headquarters units, assistant commandants for directorates, Chief Counsel and special staff offices at Headquarters shall ensure compliance with the provisions of this Manual.

3. DIRECTIVES AFFECTED. The Coast Guard Military Personnel Security Program, COMDTINST M5520.12A is canceled.

4. DISCUSSION. This Manual is the basic Coast Guard directive governing the military personnel security program. The provisions of this manual apply to all military personnel including the ready reserve and standby reserve (active status). It also applies to applicants for appointment or enlistment.

5. REQUESTS FOR CHANGES. Units and individuals may recommend changes by writing via the chain of command to Commandant (G-CFI), U.S. Coast Guard Headquarters, 2100 Second Street, S.W., Washington, DC 20593-0001.

6. FORMS AVAILABILITY. The following forms are available on Jetform Filler: Coast Guard Personnel Security Action Request (CG-5588), Classified Information Nondisclosure Agreement (SF-312), Questionnaire for National Security Positions (SF-86), Acknowledgement/Referral (CG-4217), U.S. Civil Service Commission Fingerprint Chart

DISTRIBUTION – SDL No139

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	3	2	3		2	2	1	2	1	1		1	2	1	1	1	1		1		2					
B	1	8	10	2	12	5	3	5	3	3	2	3	3	10	3	2	2	40	2	1	2	1	3	2	1	1
C	3	2	1	3	2	1	1	1	2		2	1	2	5	2		3	1	2	1	1	1	1	1		
D	2	1	1	3	11	1	1	1	1	1	1	1	1			1	1	1	1	1	1	1	1			1
E		2	1					1		1	1	1	1	1	1				1							
F																			1							
G	1	1	1	1	1																					
H																										

NON-STANDARD DISTRIBUTION:

(SF-87), Security Termination Statement (DOE Form F 5631.29). The following forms are available from Engineering Logistic Center, Baltimore: Fingerprint card (DD-2280), stock number SN-0102-LF-002-2801 U/I PG, Applicant Fingerprint card (FD-258), stock number 7530-00-F01-9400 U/I HD.

R. S. HOROWITZ
Director of Finance and Procurement

RECORD OF CHANGES

CHANGE NUMBER	DATE OF CHANGE	DATE ENTERED	ENTERED BY (Printed name and signature)

TABLE OF CONTENTS

CHAPTER 1. - PERSONNEL SECURITY PROGRAM

CHAPTER 2. - MILITARY PERSONNEL SECURITY

CHAPTER 3. - SECURITY AWARENESS AND COUNTER-ESPIONAGE

CHAPTER 4. - ADJUDICATIVE GUIDELINES

CHAPTER 5. - DEPARTMENT OF ENERGY NUCLEAR SECURITY PROGRAM "Q" CLEARANCES

CHAPTER ONE

PERSONNEL SECURITY PROGRAM

A. <u>Definitions</u>. The terms below appear throughout this Manual. They have specific meanings, some of which may differ slightly from their meanings in other contexts. Familiarity with these terms is essential to an understanding of the Coast Guard's Personnel Security and Counter-Espionage Programs.

1. <u>Access</u>. The ability and opportunity to obtain knowledge of classified information for official duties. An individual, in fact, may have access to classified information by being in a place where such information is kept, if the security measures that are in force do not prevent him from gaining knowledge of such information. Access is based upon a need-to-know determination made by the holder of the classified material and access is authorized only after the issuance of a temporary, interim or final security clearance at the appropriate level.

2. <u>Adverse action</u>. Any action taken with respect to an individual who has been investigated under the provisions of this Manual that results in:

   a. Denial or revocation of security clearance.
   b. Denial or revocation of access to classified information.
   c. Denial or revocations of a special access authorization.
   d. Nonacceptance for or discharge from the Coast Guard when any of the foregoing actions are taken as the result of a Personnel Security determination.

3. <u>Adjudication</u>. An overall common sense determination based upon consideration and assessment of all available information, both favorable and unfavorable, with particular emphasis being placed on the seriousness, recency, frequency and motivation for the individual's conduct; the extent to which conduct was negligent, willful, voluntary, or undertaken with knowledge of the circumstances or consequences involved; and, to the extent that it can be estimated, the probability that conduct will or will not continue in the future.

4. <u>Alien</u>. Any person not a citizen of the United States.

5. <u>Citizen</u>. United States citizens, either by birth or who are U. S. Nationals, those who have derived U. S. Citizenship or those who acquired it through naturalization. A person born in one of the 50 United States, Puerto Rico, Guam,

American Samoa, Northern Mariana Islands, U.S. Virgin Islands; or Panama Canal Zone (if the father or mother (or both) was or is, a citizen of the United States).

6. Classified Information. Official information or material that requires protection in the interests of national security and that is classified for such purpose by appropriate classifying authority in accordance with Executive Order 12958.

7. Clearance. A determination that a person is eligible and authorized access to classified information on a need-to-know basis under the standards of this instruction. The level of access will not exceed the level of clearance.

8. Command. For the purpose of this instruction, a Command is any organizational entity under one individual authorized to exercise direction and control. The term includes units, ships, laboratories, bases, squadron's activities, facilities or any other indication of organizational integrity.

9. Commanding Officer. Unless otherwise noted, the term "Commanding Officer" includes "Commander", "Officer-in-Charge", "Director", "Inspector" and any other title assigned to an individual, military or civilian, who through Command status, position or administrative jurisdiction, has the authority to render a decision with regard to a specific question under consideration

10. Command Security Officer (CSO). The CSO works under the direction of the Commanding Officer, who is ultimately responsible for all national security information at his/her unit. The CSO shall be a commissioned officer, chief warrant officer, senior petty officer (E-7 through E-9) or civilian employee (GS-9 or above). The commanding officer shall designate the CSO in writing with a copy to the cognizant Security Manager. Reference Classified Information Management Program (COMDTINST M5510.23 (series)).

11. Continuous Service. Continuous service refers to honorable active duty; attendance at the military academies; membership in Reserve Officer Training Corps (ROTC) Scholarship Program; Army and Air Force National Guard membership; service in the military Ready Reserve forces (including active status); civilian employment in government service, civilian employment with a Government contractor or as a consultant involving access under the National Industrial Security Program. Continuous service is maintained despite changes from one of the above statuses to another as long as there is no single break in service greater than 24 months.

12. Eligibility. Results from a determination made by a trained adjudicator under the standards of Enclosure (1), which establishes the highest level of final security clearance that an individual may qualify to receive. The determination will be based upon the type and recency of the member's personnel security investigation.

Also, eligibility can be affected by the review of any other pertinent information relating to the member's qualification for a final security clearance.

13. Foreign National. Considered to be any person not a U.S. citizen or immigrant alien. American citizens representing foreign governments, foreign private interests, or other foreign nationals are considered to be foreign nationals for the purposes of this instruction, when acting in that capacity.

14. Immigrant Alien. Any alien lawfully admitted into the United States under an immigration visa for permanent residence.

15. Interim Security Clearance. In exceptional circumstances where an employee must perform official functions requiring access to classified information prior to completion of the required investigation, the servicing security organization may grant the employee and interim security clearance pending completion of the investigation. This type of access may be granted only to particular, identified categories of classified information necessary to perform the lawful and authorized functions that are the basis for the granting of this access. This process shall not be used in lieu of a waiver or as a means to place an employee in a sensitive position without the required background investigation.

16. Level of Security Clearance. Top Secret, Secret or Confidential and indicates the highest level of classified information to which access may be granted based on that clearance if need-to-know exists.

17. Limited Access Authorization. Where there are compelling reasons in the furtherance of a unit's mission, and a certification that a person is authorized to have access only to certain specific classified information which has been carefully screened by the appropriate Security Officer for its release to that person, immigrant alien and foreign national employees who possess a special expertise may be granted limited access to classified information only for specific programs, projects, contracts, licenses, certificates, or grants for which there is a need for access to Confidential and Secret information only. Such individuals shall not be eligible for access to any greater level of classified information than the United States Government has determined may be releasable to the country of which the subject is currently a citizen, and such limited access may be approved only if the prior 10 years of subject's life can be appropriately investigated. If there are any doubts concerning granting access, additional lawful investigative procedures shall be fully pursued.

18. Minor Derogatory Information. Information that by itself, is not of sufficient importance or magnitude to justify an unfavorable administrative action in a personnel security determination.

19. Major Derogatory Information. Information that could, in itself, justify an unfavorable administrative action, or prompt an adjudicator to seek additional investigation or clarification.

20. National Security. The national defense and foreign relations of the United States.

21. Need-to-Know. A determination made by the possessor of classified information that a prospective recipient, in the interest of national security, has a requirement for access to the information in order to perform tasks or services essential to the fulfillment of an official United States Government program. Knowledge, possession of, or access to, classified information shall not be afforded to any individual solely by virtue of the individual's office, position, or security clearance.

22. One-Time Access. Member must be a U.S. citizen, must have a current security clearance. The access must be at the next higher level. The person must have been employed in the military, civilian or contractor capacity for the last two continuous years. If the person has had a break in service, employment, or contract status within the last two years, then these procedures cannot be used. The procedure applies to full-time personnel only. The access must be limited to one or just a few times. If the person will require access on a recurring basis, process him or her for the higher level clearance. One-time access can be used up to 90 days.

23. Personnel Security Investigation **(**PSI**)**. Any investigation required for the purpose of determining the eligibility of military and civilian personnel, contractor employees, consultants, and other personnel affiliated with the Coast Guard, for access to classified information, acceptance or retention in the Armed Forces, assignment or retention in sensitive duties, or other designated duties requiring such investigation. PSI's include investigations of affiliations with subversive organizations, suitability information, conducted for the purpose of making personnel security determinations. They also include investigations of allegations that arise subsequent to adjudicative action and require resolution to determine an individual's current eligibility for access to classified information or assignment or retention in a sensitive position

24. Presidential Support Activities. Coast Guard Personnel assigned to the President and Vice President as Military Social Aides, to White House communications activities and the Presidential retreat, to the Office of the Vice President, Honor Guard personnel, Ceremonial units and military bands who perform at Presidential or Vice Presidential functions and facilities and personnel in designated units requiring a lessor degree of access to the President or Vice President are considered assigned to Presidential Support Activities.

25. Sensitive Compartmented Information (SCI). All information and materials bearing special intelligence community controls, indicating restricted handling within intelligence collection programs and their end products. These special community controls are formal systems of restricted access established to protect the sensitive aspects of sources and methods and analytical procedures of foreign intelligence programs.

26. Sensitive Position. Any position so designated within the Department of Transportation, the occupant of which could bring about, by virtue of the nature of the position, a materially adverse effect on the national security. All DOT civilian positions that are sensitive positions are designated as noncritical-sensitive, critical-sensitive, or special-sensitive.

27. Special Access Program. Any program imposing "need-to-know" or access controls beyond those normally provided for access to Top Secret, Secret or Confidential information. Such a program includes, but is not limited to, special clearance, adjudication, investigative requirements, material dissemination restriction, or special lists of persons determined to have a need-to-know.

28. Temporary Access. Temporary eligibility for access may be granted when there is a need for an employee to have this access for a limited period of time, such as for one-time participation in a classified project. The access may be granted to an individual who has met the requirements for an interim or final clearance, except that only COMDT (G-CFI) may grant a temporary Top Secret clearance if the person does not have a current SSBI. Temporary access is not to exceed 60 days; but, if circumstances warrant, may then be extended for an additional period of time not to exceed a total of six months. The command shall establish a fixed date or event for expiration of the access. The access granted shall be limited to information related to a particular project or assignment.

29. U. S. National.

    a. A person born in an outlying possession of the United States on or after the date of formal acquisition of such possession or;

    b. A person born outside the United States and its outlying possessions of parents both of whom are nationals, but are not citizens of the United States, and have had residence in the United States or one of its outlying possessions prior to the birth of such person; or

    c. A person of unknown parentage found in an outlying possession of the United States while under the age of five years, unless shown, prior to attaining the age of 21 years, not to have been born in such outlying possession. For the purposes of this instruction, U.S. Nationals are included in the use of the term "U.S. Citizens".

B. Basic Policies.

1. The Department of Transportation (DOT) is responsible for issuance of departmental policy for the Coast Guard to follow in the management and operation of the Military Personnel Security Program. Additionally, it directs, insofar as practicable, that operations shall be compatible with those of the DoD and DOT to facilitate the transfer of the Coast Guard to the Navy, if directed. Where possible, this Manual parallels the guidance provided by various Navy and DOT Instructions.

2. This Manual provides authority and necessary guidance for the management and administration of the Coast Guard Military Personnel Security and Counter-Espionage Programs. It provides guidance on personnel security investigation, adjudications, determinations, clearance, access to classified information, and the termination of clearances due to adverse suitability factors.

C. Applicability.

1. The personnel security policies and procedures in this Manual apply primarily to eligibility for access to classified information or assignment to sensitive duties that are subject to investigations under provisions of this Manual. This Manual is not the authority to deny or terminate military service unless loyalty is the central issue.

2. The personnel security policies and procedures for specific programs, such as the Industrial Security Program, are found in instructions governing those programs.

D. Authority and Jurisdiction.

1. The Coast Guard Military Personnel Security Program operates under the authority, provisions and guidance of DOT Order 1630.2(series), DOT Personnel Security Management.

2. Coast Guard military personnel security operations shall apply the standards and criteria of DOT Order 1630.2(series). Insofar as practicable, the operations shall be compatible with those of the DoD and DOT to facilitate Coast Guard transfer to DoD, if directed.

3. The Director, Office of Security and Administrative Management, DOT, will periodically evaluate and report on the effectiveness of the Coast Guard Military Personnel Security Program.

4. The Chief, Office of Security Policy and Management, Commandant (G-CFI), is the Director of Coast Guard Security, and serves as the program manager for the

Coast Guard Security Program, the Personnel Security and Counter-Espionage elements of the security program, and serves as the President of the military Personnel Security Appeals Board (PSAB).

5. The Department of Transportation's Transportation Administrative Service Center (TASC) Security Operations Division (hereafter referred to as the Central Adjudication Facility (CAF) through a memorandum of agreement, is contracted by the Coast Guard to manage and operate a Coast Guard oriented Central Adjudication Facility. The CAF will act as the Coast Guard's central source for final Coast Guard personnel security clearances. TASC has the authority to grant, revoke or deny all security clearances for military personnel, and to grant, and recommend to Commandant (G-CFI) the revocation or denial of all other Coast Guard security clearances. Commandant (G-CFI) is the final authority for the revocation or denial of Coast Guard civilian employee, contractor employee, or Auxiliary personnel security clearances.

6. Commandant (G-OCI) is responsible for the management of access to Sensitive Compartmented Information (SCI).

7. For access other than SCI, Commanding Officers of an active duty unit may grant an interim security clearance or temporary access to military personnel subject to the Commanding Officer's authority and to the relieving Officer upon the change-of-command. The Commanding Officer granting the interim clearance or temporary access shall be eligible for a security clearance equal to or higher than the interim clearance or temporary access being authorized. When it is impracticable for a departing Commanding Officer to grant an interim clearance to the relieving Officer, the interim clearance may be granted by the Executive Officer. The Command Security Officer may be designated the authority to grant interim security clearances or temporary access provided they are eligible for a security clearance at the appropriate level.

8. District Commanders or an individual designated by the District Commander may grant interim clearance or temporary access to drilling reserve personnel not on extended active duty, under their jurisdiction.

9. All personnel designated as an authority to grant interim security clearances or temporary access to classified information shall be properly trained in the review of completed Standard Forms 86 and in the review and evaluation of data regarding previously completed investigations.

E. <u>Responsibilities</u>.

1. Upon a new member arriving at a unit, Commanding Officers shall ensure that the member's need for a security clearance/access is reviewed.

2. Commanding Officers shall ensure that all personnel assigned to duties requiring access to classified information are initially indoctrinated and periodically instructed thereafter on the national security implications of their duties and their individual responsibilities.

3. Procedures shall be established, and special counseling made available in an effort to encourage individuals granted a clearance under this Manual to seek appropriate guidance and assistance on any personal problem or situation that may have a bearing on their security clearance eligibility.

4. Individuals must familiarize themselves with pertinent security instructions that pertain to their assigned duties. Further, individuals must be aware of the standards of conduct required of persons holding a security clearance. In this connection, individuals must recognize and avoid the kind of personal behavior that would result in rendering one ineligible for a security clearance. In the final analysis, the ultimate responsibility for maintaining continued eligibility for a security clearance rests with the individual. All personnel employed in and by the Coast Guard holding a security clearance are subject to the national investigative and adjudicative standards for access to classified material or assignment to sensitive duties. All personnel subject to the personnel security program are responsible for reporting derogatory information via their chain of command.

F. <u>Citizenship</u>.

1. Only United States citizens are eligible for security clearances. Only United States citizens are eligible for assignment to sensitive duties or access to classified information unless there are compelling reasons in the furtherance of national security or Coast Guard missions, including special expertise, to assign a non-U.S. citizen to sensitive duties or to grant a Limited Access Authorization. When this Manual refers to U.S. Citizenship, it makes no distinction between those who are U.S. citizens by birth, those who are U.S. nationals, those who have derived U.S. citizenship or those who acquire it through naturalization. This manual identifies "Non-U.S. citizens" as immigrant aliens and foreign nationals. Immigrant aliens are those who have been lawfully admitted to the U.S. under an immigrant visa for permanent residence. Foreign nationals are those who are not U.S. citizens, U.S. nationals or immigrant aliens to the United States.

   a. <u>Dual Citizenship</u>: We may not predetermine that a person with dual citizenship status is automatically ineligible for access to classified information and we may not have in place any procedure that denies such a person a security clearance without due process. The appropriate guideline is Guideline C, Foreign Preference, of the Adjudicative Guidelines (Chapter Four of this manual) for Determining Access to Classified Information. Guideline C states that the exercise of dual citizenship is a condition that could raise a concern

and may be disqualifying. It is definitely a concern when the individual has, at any time during at least the last 10 years, taken steps to maintain or exercise the benefits of another country's citizenship. However, Guideline C also lists conditions that could mitigate concerns in cases involving dual citizens, such as dual citizenship based solely on parents' citizenship or birth in a foreign country, and an individual's willingness to renounce dual citizenship.

b. When dual citizenship is an issue, we must ensure that we have sufficient information to complete the adjudication process; and we must provide the individual an opportunity to respond to all pertinent information we have regarding the dual citizenship before denying or revoking a security clearance. We must then apply Guideline C in evaluating any mitigating information the person furnishes before taking any final denial or revocation action.

2. Under no circumstance will non-U.S. citizens be eligible for access to sensitive compartmented information, classified NATO information, COMSEC keying material, cryptologic information, intelligence information (unless authorized by the originator) or any other special access program. Enlisted non-U.S. citizens may not enter ratings, which generally require access to classified information. (See Personnel Manual, COMDTINST M1000.6 (SERIES)).

3. United States citizenship must be verified prior to granting a security clearance.

G. <u>Personnel Security Data Management</u>. Personnel security records contain considerable, highly privileged information and, in some cases, classified information. It is imperative that these records be carefully protected in their handling, transmittal, release and storage.

1. Freedom of Information Act (FOIA) or Privacy Act (PA) requests for investigative information must be addressed to the agency conducting the investigation. Release of investigative information obtained under a pledge of confidence shall be controlled in accordance with the commitment made by the investigative agency concerned. Normally this commitment would preclude divulging it to the person investigated.

2. Medical reports obtained in conjunction with an investigation shall be carefully controlled to ensure that the privileged, personal information is not divulged to persons without a need-to-know who do not need it for security or suitability determination.

3. Classified investigative reports shall be protected as required by Coast Guard instructions regarding control and safeguarding of classified information.

4. Records must be kept in lockable cabinets, safes or Automated Information Systems (AIS) accredited in accordance with Automated Information Systems

Manual (COMDTINST M5500.13 (series)). Access must be controlled to work areas where records are maintained. Positive identification and a need-to-know are required for users of these records.

H. **Foreign Assignments and Foreign Travel**. Special safeguards are required to protect national interests and national security information when Coast Guard personnel and representatives are given foreign assignments or perform official foreign travel. For this purpose, a "foreign" location means outside the 50 States, the District of Columbia, or any of the United States possessions, territories or trust territories. Investigative requirements and security precautions specified below are applicable.

1. Coast Guard officials designating persons for foreign assignments shall carefully screen each designee to ensure that presence of the person in the foreign country is not adverse to the interests of the United States.

2. When the assignment will not exceed 1 year, there are no special investigative requirements other than those applicable to the sensitivity and duties of the position.

3. Coast Guard personnel assigned official travel in a foreign country must exercise good judgment at all times to ensure that nothing contrary to the interests of the United States or the Coast Guard is done. Officials authorizing the travel are responsible for ensuring that each traveler possesses good character and the reliability needed for the assignment. Investigative requirements for similar duties at a domestic location are applicable, except for the following:

   (a) Heads of Delegations. Any person from the Coast Guard selected to head a delegation from the United States to an international conference on other than a one-time basis must have been the subject of a Single Scope Background investigation within the last 5 years.

   (b) Nominee as Coast Guard Representative at International Conference. Nomination to represent the Coast Guard at an international conference is subject to the completion of a favorable NACLC or a more comprehensive investigation. Normally, an investigation has been conducted on Federal employees, but nomination of technical advisors from the transportation industry requires special action. At least 4 weeks prior to the international conference, the Coast Guard office arranging for the services of the industry technical advisor shall furnish to Commandant (G-CFI) the information and papers needed for processing the NACLC investigation.

   (c) Reference the Personnel Manual (COMDTINST M1000.6 (series)) for other areas of concern when traveling abroad.

I. Assignment to Presidential Support Activities.

1. Commandant (G-CFI) is the program manager and final Coast Guard authority for assignment to Presidential Support Activities (PSA) and access to the White House.

2. The policies and procedures for evaluation of military and civilian personnel assigned to Presidential Support Activities are contained in Selection of Department of Defense Military and Civilian Personnel and Contractor Employees for Assignment to Presidential Support Activities (DoD directive 5210.55 (series)).

3. The adjudicative standards contained in section four of this manual will be used to ensure that only the most suitably qualified candidates are considered for nomination to Presidential Support Duties.

4. Presidential Support Activities are designated as Category One, Category Two and Category Three. A complete listing of personnel in each category is contained in DoD directive 5210.55(series). Normally, Coast Guard personnel will fall into the following categories:

   a. **Category One**: Military Aides to the President or Vice President

   b. **Category Two**: Military Social Aides, Personnel assigned to White House Communications activities and Presidential retreat duties in support of the President or Vice President.

   c. **Category Three**: Personnel assigned to honor guard units, ceremonial units, and military bands who perform at Presidential or Vice Presidential functions and facilities.

5. Personnel nominated for Category One or Category Two duties must have been the subject of a Single Scope Background investigation (SSBI) within the 36 months preceding selection. The individual's spouse or cohabitant shall be, at a minimum, the subject of a National Agency Check (NAC). If the individual marries subsequent to completion of the SSBI, the required NAC shall be conducted at that time.

6. Personnel nominated for Category Three duties must have a favorable NAC, local agency check, and credit check (NACLC) within the last 36 months preceding selection for Presidential support duties.

7. Once the required clearance has been granted, Commandant (G-CFI) will conduct suitability adjudication for White House Access in accordance with Selection of Department of Defense Military and Civilian Personnel and Contractor Employees for Assignment to Presidential Support Activities (DoD directive 5210.55(series)). If an investigation contains derogatory information that would result in denial of assignment to PSA, a letter will be sent to the member via the member's Command offering the member an opportunity to explain, refute, mitigate or provide information. If necessary, a limited inquiry may be requested from Commandant (G-O-CGIS) to further investigate the derogatory information. Commandant (G-CFI) will then complete the adjudication process and make a final determination on behalf of the Commandant. There is no appeals process associated with a final denial of eligibility determination by Commandant (G-CFI) or the White House Military Office, Security Advisor.

8. The administrative nickname "YANKEE WHITE" shall be stamped or printed in bold letters across the top of all CG-5588's pertaining to Presidential Support Activities nominees.

J. <u>Program Evaluation</u>. From time to time it is essential for commands to evaluate their individual military personnel security programs to ensure that all established procedures are complied with. Commands and security managers will use enclosure (2) to this manual when evaluating individual command military personnel security programs. Commands will conduct a self-evaluation each year and correct any discrepancies noted. Copies of the evaluation will be submitted to the cognizant security manager.

CHAPTER TWO

MILITARY PERSONNEL SECURITY

A. General.

Military personnel security policies and procedures in this manual apply to eligibility for access to classified information. In order to be eligible for access to classified information or assignment to sensitive duties an individual must meet the following criteria.

a. Have the appropriate Personnel Security Investigation.

b. Has been determined eligible by the Central Adjudication Facility.

c. Be granted access by the Commanding Officer or designated official.

d. Execute a non-disclosure agreement (SF-312).

e. Possess a valid need-to-know.

B. Personnel Security Investigation.

1. A personnel security investigation (PSI) is an inquiry by an investigative agency, authorized to conduct investigations, into an individual's activities, for the specific purpose of making a personnel security determination

2. The U.S. Security Policy Board (USSPB) in accordance with Executive Order 12968 established standard investigative guidelines, which are approved by the President for use by all federal government agencies. The current investigative standards are contained in Enclosure (1) of this manual. There are three investigations conducted for the purposes of determining security clearance eligibility. The Coast Guard Investigative Service (G-O-CGIS), as a service to the Office of Security Policy and Management (G-CFI) conducts personnel Security Investigations. These investigations are:

    a. Single Scope Background Investigation (SSBI)

    b. Single Scope Background Investigation- Periodic Reinvestigation (SSBI-PR)

c. National Agency Check with Local Agency Check and Credit Check (NACLC)

C. <u>Security Clearance and Eligibility Determination</u>.

1. Once the Personnel Security Investigation is completed, it is forwarded to the Central Adjudication Facility (CAF). The CAF reviews the information in the Personnel Security Investigation and compares it to nationwide adjudication standards. These standards are contained in chapter 4 of this manual. The adjudicator will then determine whether or not the individual is eligible for a security clearance.

2. A personnel security clearance is an administrative determination that an individual is <u>eligible</u> for access to classified information or assignment to sensitive duties at a specified level.

3. To be eligible for a security clearance, assignment to sensitive duties or access to classified information, the following requirements must be met:

   a. <u>Top Secret</u>: Member must have been the subject of a favorably adjudicated SSBI. If more than five years old, a periodic reinvestigation must have been requested. There can not be a break in service of more than 24 months, the member must have properly executed an SF-312 non-disclosure agreement and completion of a local records check (LRC) must be documented on CG-5588.

   b. <u>Secret</u>: Member must have been the subject of a favorably adjudicated NACLC (or SSBI), which is less than 10 years old. If more than 10 years old, a NACLC update must have been requested. A NACLC update is simply a new NACLC request; however, a notation "NACLC update" and the reason a secret clearance is required should be in the remarks section of the CG-5588. There can not be a break in service of more than 24 months, the member must have properly executed an SF-312 non-disclosure agreement and completion of a local records check (LRC) must be documented on CG-5588. If an individual has a favorably adjudicated NAC or ENTNAC completed prior to 1 October 1997 that is less than 10 years old it to is acceptable for up to a Secret clearance. All new clearances granted must be based on investigations meeting the current standards. The NAC or ENTNAC is not acceptable as a basis for granting a new security clearance.

c. Confidential: Member must have been the subject of a favorably adjudicated NACLC, which is less than 15 years old. If more than 15 years old, a NACLC update must have been requested. There can not be a break in service of more than 24 months, the member must have properly executed an SF-312 non-disclosure agreement and completion of a local records check (LRC) must be documented on CG-5588.

D. **Access**. The ultimate authority for granting access to classified information rests with the Commanding Officer responsible for the security of the information or material at his/her command. A Commanding Officer may grant access to classified information to an individual who has an **official need to know**, a valid security clearance, has a properly executed a SF-312 on file and there is no locally available unfavorable information.

1. If significant derogatory information is discovered after the PSI and clearance determination, access will be suspended following the guidelines set forth in paragraph 2.V. of this chapter. If access has not been suspended at the command level, Commandant (G-CFI) may direct that access be suspended pending resolution.

2. The number of personnel that a command grants access to classified information shall be kept to the **absolute minimum** required for the conduct and performance of national security and Coast Guard missions.

3. An individual's access history will be maintained at the command level for a period of four years after transfer, discharge or retirement. The Command Security Officer (CSO) will maintain a roster of all personnel assigned to their command who have been granted access to classified material. The roster will contain the following information:

   a. Name, rank and SSN

   b. Type of investigation

   c. Date investigation was completed

   d. Level of final clearance granted

   e. Expiration date for interim or temporary clearance

   f. Reason top secret access is/was required (if applicable)

   g. Date access granted/terminated

h. Date SF 312 (non-disclosure agreement) was executed

4. Access shall not be granted solely to permit entry to, or ease of movement within, controlled areas when the individual has no need for access and access to classified information may be reasonably prevented.

5. Access will not be granted to persons who may only have inadvertent exposure to sensitive or classified information.

6. Personnel shall not be granted access to classified information merely as a result of any particular title, rank, position, or affiliation. (Security managers with the appropriate credentials shall be authorized access in the performance of their duties).

E. **Security Clearance Re-approval**.

1. When an individual is transferred from a command, his/her requirement for access at that command no longer exists. Their access is therefore withdrawn even though their clearance remains unchanged.

2. Executive Order 12968 requires that all security clearances be re-approved whenever a member with a security clearance is transferred if there is a need for access. Therefore, the member's new Commanding Officer (or a person designated in writing by the Commanding Officer) will sign a CG-5588 re-approving the individual's clearance. See exhibit 2-1 for re-approval instructions.

3. Once a clearance is re-approved, commands may grant access provided the following conditions are met:

   a. Access is only required at or below the level of clearance eligibility.

   b. The previously issued Central Adjudication Facility (CAF) source document or appropriate Coast Guard Human Resources Management System (CGHRMS) entries are sighted. Source document and CGHRMS extracts should be on file in the individuals PDR.

   c. A thorough local records check is conducted.

   d. A SF-312 has been properly executed and a copy is on file in the member's PDR.

F. **Investigative Request Procedures**. Investigation packages are to be forwarded to G-O-CGIS via first class mail only. Forwarding investigation packages via

overnight delivery is discouraged as it causes delay in processing. All personnel security investigations shall be completed within twelve months of receipt by the investigating agency in receipt of the investigation package. Deviation from this requirement must be approved by Commandant (G-CFI), in writing. Requests for personnel security investigations will be processed as follows:

1. National Agency Checks with Local Agency Checks and Credit Check (NACLC). CG-5588 (1 original), SF-86 (1 original, 1 copy with original signatures), a self addressed CG-4217 (or locally produced equivalent (include a self addressed envelope)), FD-258 (2 original), and 2 original signed DOT 1631 will be completely reviewed by the Command Security Officer and **forwarded to Commandant (G-O-CGIS)** to conduct the NACLC. Commands are reminded that Entrance National Agency Checks (ENTNAC) are conducted on all first term enlistees and are not valid for a security clearance unless the ENTNAC was conducted prior to 1 October 1997. Beginning 01 October 2003, ENTNAC's will no longer be valid for the issuance of a security clearance. After 1 October 1997, all clearances are to be based on investigations meeting the current investigative standards.

2. Single Scope Background Investigations (SSBI). CG-5588 (1 original), SF-86 (1 original, 1 copy with original signatures), a self addressed CG-4217 (or locally produced equivalent (include self addressed envelope)), FD-258 (2 originals), 2 original signed DOT 1631, and if not included on previous investigation; SF-86 (1 original and 1 copy with original signature by member (and spouse and/or cohabitant, foreign born children over age 18 and foreign born parents) when requesting SCI eligibility. Member must sign; spouse, foreign-born children over age 18 and foreign-born parents signatures are optional). Item 1-8 must be completed for these members for SCI eligibility only will be forwarded to the cognizant Security Manager after complete review by the Command Security Officer. Since the number of personnel with Top Secret clearance will be kept to an absolute minimum, justification for the SSBI will be noted in the remarks section of the CG-5588 including the Billet Control Number of the subject's present billet or future billet if being transferred. The cognizant Security Manager will submit the package to Commandant (G-O-CGIS) to conduct the SSBI.

3. Scope. Some of the questions on the revised SF-86 specify a time frame of 7 years, which is not consistent with National Security Directive (NSD) 63 which requires a **10 year scope for SSBI's**, (the scope for PR-SSBI's is 10 years or to the date of the last completed SSBI) therefore, when completing SF-86 for a SSBI, the following questions will be answered with a 10 year scope. Forms received not meeting these requirements will be returned without action:

a. Question 9, Residences

b. Question 10, Schools

c. Question 11, Employment Activities

d. Question 12, References

e. Question 21, Medical

f. Question 22, Employment Record

g. Question 23, Police Record

h. Question 29 Court Actions

Note: The scope for all questions when requesting a NACLC is 7 years or to the 18th birthday, whichever is less. Ensure the ORI on the FD-258 (fingerprint card) reflects "DCCG00100, US COAST GUARD, WASH, DC".

4. When a security clearance is required to meet urgent operational commitments, ships that are scheduled to be underway may request message notification of clearance by indicating on the CG-5588 "message response requested".

5. The CSO will maintain a copy of the member's SF-86 until the investigation has been completed. If the member is transferred before the investigation is completed, the CSO will forward the copy to the CSO of the receiving command. This will facilitate review by the command or subsequent commands if interim clearance is necessary.

6. Cancellation. When a personnel security investigation is in a pending status and circumstances change that negates the need for the investigation, the member's command will immediately advise their cognizant security manager and provide the reason for cancellation.

G. Interim Security Clearance. An interim security clearance is granted temporarily, pending completion of full investigative requirements. Interim clearances are granted by authority of the Commanding Officer and will be recorded on the CG-5588 (see paragraph 2-M). Prior to granting interim clearance, commands shall ensure that the member has a properly executed SF-312 on file.

1. Interim Confidential/Secret.

a. Conduct a local records check of unit Personnel Data Record (PDR), medical record and any locally maintained training files.

Perform a CGHRMS data base check for possible existing security clearance eligibility.

b. Review the member's completed Questionnaire for National Security Positions (SF-86), ensure that all information required is provided and complete. If unfavorable information is contained in the SF-86, interim clearance may not be granted without adjudication of the completed investigation by the central adjudication facility (CAF). Contact your cognizant security manager for further determination.

c. If the local records check and the SF-86 contain no unfavorable information, and there is no security clearance data on the member in CGHRMS, the interim clearance may be granted upon submission of a NACLC request to Commandant (G-O-CGIS) with justification.

d. The interim clearance is valid pending completion of full investigative requirements.

2. Interim Top Secret.

a. Conduct a LRC of unit personnel data records, medical records and any locally maintained training files. Conduct a CGHRMS check for possible existing security clearance eligibility.

b. Review the member's completed Questionnaire for National Security Positions (SF-86), ensure that all information required is provided and complete. If unfavorable information is contained in the SF-86, an interim clearance will not be granted without adjudication of the investigation by the CAF. Contact your cognizant security manager for further determination.

c. Review the Questionnaire for National Security Positions (SF-86) completed for spouse and/or cohabitant and foreign-born parents and/or children over age 18 for SCI eligibility only.

d. Review the Coast Guard Human Resource Management System (CGHRMS) and ensure that a favorable personnel security investigation of any type has been completed within the last 10 years

e. If the LRC and the SF-86 result in favorable review and the prior investigation was adjudicated favorably with no break in service

exceeding 24 months since the investigation was completed, an Interim clearance may be granted.

f. Forward the investigation package to the cognizant Security Manager, ensuring that thorough justification for an SSBI is in the remarks section of the CG-5588. The cognizant Security Manager will review the package for correctness, certify the justification and submit the package to Commandant (G-O-CGIS).

g. The Interim Top Secret clearance is valid for a period not to exceed 6 months.

h. If the LRC and the SF-86 result in favorable review, and, after contacting the cognizant security manager a prior investigation cannot be confirmed or does not exist, the Central Adjudication Facility (CAF) must grant the interim clearance. Submit a message action to CAF, information to Commandant (G-CFI) and the cognizant security manager, containing the following information:

(1) Member's name/rate/rank

(2) Member's SSN

(3) Member's date and place of birth

(4) Name of person conducting *favorable* review of LRC and SF-86

(5) Date SSBI package submitted to cognizant security manager.

(6) Reason interim Top Secret clearance is necessary

H. **<u>Extension of Interim Security Clearance</u>**. If a final Top Secret security clearance is not received and no unfavorable information has been developed locally, the Commanding Officer may request an extension of the interim security clearance by submitting a CG-5588 to the Central Adjudication Facility (CAF). This extension process may continue until final determination has been received from the CAF. Note the extension on the original CG-5588 used to grant the interim clearance. The cognizant security manager will be notified of any interim clearance, which has been in effect for more than 06 months.

I. **<u>Granting Interim Security Clearance When the SF-86 Cannot Be Reviewed</u>.** If a member granted an interim security clearance is transferred prior to the completion of the full investigative requirements, the receiving command may utilize the previous commands interim decision to grant an interim clearance, provided no new derogatory information is discovered or revealed in the local

records check. Commands should note on the CG-5588 that the SF-86 was not reviewed and the interim clearance was granted based on the previous commands review of the SF-86. Both CG-5588's should be maintained until the investigation is completed and final clearance eligibility is made by the CAF.

J. <u>Clearance Based on an Investigation From Another Agency</u>.

1. If there is no current Coast Guard investigation on file, but the command has evidence that an investigation was conducted by another agency, that investigation may be used as a basis for granting the clearance if the investigation is within scope, was favorably adjudicated, provides the same coverage as the Coast Guard investigation and there was no break in service over 24 months since the investigation was completed. Submit a CG-5588 and annotate the type of investigation and the agency that conducted it in the remarks block. Attach any source document or certificate of clearance from the other agency if available and submit to Commandant (G-CFI).

2. If the prerequisite investigative requirements cannot be obtained, then a new investigative request for the appropriate clearance level must be forwarded to the Commandant (G-O-CGIS) (via the cognizant Security Manager if an SSBI or SSBI (PR) is requested). The requesting command may issue an interim clearance to meet the unit's operational needs, following the Interim Security Clearance procedures in this Manual.

K. <u>Coast Guard Personnel Assigned to Other Components</u>. Coast Guard personnel assigned to another service often require a security clearance. Normally, the command with administrative control of a member assumes the administrative responsibility of security clearance processing. The cognizant security manager shall ensure that the appropriate security clearance determination is made and the other activity is notified accordingly. If an investigation is required, all investigative paperwork will be completed by the member and submitted to the command with administrative control for review and submission to Commandant (G-O-CGIS). SSBI's shall be forwarded to the cognizant security manager for final review prior to forwarding to Commandant (G-O-CGIS).

L. <u>Clearance Notification When Visiting Another Command</u>.

1. When a Coast Guard member is visiting another command (Coast Guard or other) notification of the member's clearance level may be required.

2. An official letter from the member's command to the command being visited will be sent and must indicate the following:

   a. Member's name (last, first, middle).

b. Member's rank/rate.

c. Member's SSN (last 4 digits).

d. Member's clearance level (final/interim).

e. Basis of clearance (NAC, SSBI) and date completed.

f. Date member executed the SF-312.

3. In cases where time will not allow an official letter to be received, message/fax notification may be made provided it contains the above information.

4. Hand carried clearance information is not authorized.

M. <u>Coast Guard Form 5588</u>.

1. A CG-5588 will be used to request security clearances, re-approve a clearance, grant an interim clearance, document that an interim security clearance is extended, for follow-up, and to report derogatory information or status change (i.e., upgrades and downgrades of access). Exhibit 2-2 shows an example of a CG-5588.

2. To ensure uniform submission of information and timely response, other locally produced forms or letters will not be accepted. It is vital that all requested information on the CG-5588 be completed. Incorrect or incomplete forms will result in delay of action, as the forms will be returned to the originator for resubmission.

3. As this form is used for a number of different actions, the following is a guideline for proper completion:

a. Clearance re-approval. Complete items 1 thru 8, 12 thru 15, 18 and 26.

b. Interim clearance. Complete items 1 thru 8, 12 thru 15, 16 or 17 (as appropriate) and 26.

c. Granting access. Complete items 1 thru 8, 12 thru 15, 18 and 26.

d. Requesting PSI and clearance determination. Complete items 1 thru 8 (1 thru 11 if the request is for SCI) 12 thru 15, 20 thru 21 and 24 thru 26.

e. Reporting derogatory information. Complete items 1 thru 8, 24 and 26. (Note type of report i.e. **INITIAL**, **INTERIM** or **FINAL** and provide details in block 24). Additional sheets may be used if necessary.

f. Interim clearance extensions. Note "interim clearance extended until (date)" and initial in item 24 of the CG-5588 originally granting the interim clearance.

N. Central Adjudication Facility Procedures.

1. Commandant (G-CFI) forwards all completed investigations to the Central Adjudication Facility (CAF) for adjudicative action. The CAF will make personnel security determinations based on the highest eligibility the investigation will support and grant the clearance identified on the CG-5588.

2. The CAF will make clearance notifications via CGHRMS updates and a certificate of clearance issued to the requesting command.

3. Coast Guard Reserve Personnel in an active status may be issued security clearances when necessary. The unit will request the clearance where the individual is administratively assigned. All investigative and documentation procedures remain the same as for active duty personnel.

O. Administrative Procedures.

1. Certificate of Clearance. When the Central Adjudication Facility (CAF) makes a favorable security determination, notification is made via CGHRMS updates and a certificate of clearance known as the source document. This source document shall have a properly executed SF-312 and CG-5588 attached and filed in the members PDR.

2. Periodic Reinvestigation and Investigation Updates. An investigation must be updated from time to time as part of the Continuous Evaluation Program (CEP), for those personnel who require access to classified information. The time periods for Periodic Reinvestigations (PR) and Investigation Updates depend upon the level of clearance. Time periods are contained in para 2.C.3. of this chapter. The requirement to conduct a periodic reinvestigation or an investigation update does not have an effect on an initial clearance determination unless the member has a break in service of over 24 months or the eligibility is revoked by the CAF. It is

not necessary to lower clearance or grant an interim clearance because the investigation may be past the required update or reinvestigation date unless the member fails to submit the required paperwork for the reinvestigation or update within 30 days of the clearance re-approval.

3. Clearance/Access Briefing. Each person who is granted access to classified information will be given a Clearance/Access brief prior to granting the actual access. The briefing shall be conducted in accordance with chapter three of this manual.

4. Investigations Update. The Command Security Officer will review the monthly Coast Guard Human Resources Management System (CGHRMS) control report to ensure that updated investigations are requested in a timely manner on all personnel who still require access to classified information.

5. Transfer Briefings. When individuals are transferred they must be given a transfer briefing in accordance with chapter three of this manual. This briefing is required regardless of whether or not the individual had access at the command as the individual may have had inadvertent access to sensitive information.

6. Final Termination Briefing. All personnel departing Coast Guard service, or personnel whose clearance is revoked by the CAF, will be given a final termination briefing in accordance with chapter three of this manual. This briefing is required regardless of whether or not the individual had access at the command as the individual may have had inadvertent access to classified or sensitive information. Final termination briefings are documented by completing the Security Debriefing Acknowledgement section of the SF-312, and forwarding the completed form to Personnel Command (CGPC-Adm-3) for inclusion in the member's permanent record.

7. Disposition of old Personnel Security Record (CG-5274).

   a. The CG-5274, Personnel Security Record is obsolete.

   b. All CG-5274's will be forwarded to Personnel Command (CGPC-adm3) for inclusion in the member's permanent record. Ensure all previous source documents and SF-312 copies are removed and retained in the individuals PDR.

P. Unfavorable Personnel Security Determinations.

1. When the Central Adjudication Facility (CAF) makes an unfavorable personnel security determination, action to deny or revoke security

clearance or eligibility is initiated. A Letter of Intent (LOI) listing the disqualifying factors will be forwarded to the subject via their Commanding Officer, with copies to Commandant (G-CFI) and the cognizant Security Manager. The Command Security Officer shall notify the cognizant Special Security Officer (SSO) of the LOI if SCI access is involved. A form letter acknowledging receipt of the LOI will also be enclosed. Commands shall ensure that the acknowledgment is signed by the member and forwarded to the CAF with a copy to Commandant (G-CFI) and the cognizant Security Manager. When the acknowledgement is received, the CAF will make a final determination and advise the individual via the Commanding Officer and Commandant (G-CFI). If the final decision is favorable, a copy of the notification will be forwarded to Commandant (G-CFI) and the cognizant Security Manager. If the final decision results in a denial or revocation, the subject will be advised of his/her rights by letter from the CAF via Commandant (G-CFI) and the Commanding Officer. A copy will be forwarded to the cognizant Security Manager. The CAF will forward all pertinent paperwork to Commandant (G-CFI) for insertion into the members Security File.

2. In order to appeal an unfavorable decision issued by the Central Adjudication Facility (CAF), Coast Guard personnel must first file an appeal with the Coast Guard Personnel Security Appeals Board (PSAB). The PSAB is established under the authority of the Commandant and is the sole Coast Guard appellate authority for unfavorable personnel security determination appeals by Coast Guard personnel. If the PSAB decision is adverse, the individual may appeal the decision to the Department of Transportation Personnel Security Review Board (PSRB) for a final decision.

   a. Failure of an individual to submit an appeal within the prescribed time allotted to the PSAB or an indication of intent not to appeal will result in the security determination becoming a final decision. If a member declines appeal they shall be counseled by the command on the effect of this decision on their future eligibility to remain in or apply for ratings or assignment requiring a security clearance.

   b. Requests for extensions to file an appeal will be granted only for good cause and must have a command endorsement. Submission of a request for an extension does not automatically authorize a delay in the filing of an appeal beyond the normal time limits. Appeals postmarked more than 30 calendar days after the date the individual signed the notification of a final security determination notification will be rejected as untimely. The appellant will be

notified of the decision on his/her request for an extension via their Commanding Officer.

c. Commandant (G-CFI) will appoint no less than six military officers, 0-4 or above, to serve as members of the PSAB when selected.

d. Each PSAB will be comprised of no less than three members. The Coast Guard Director of Security, Commandant (G-CFI) will serve as the President and will select two or more appointed officers to serve on each PSAB as necessary.

e. Commandant (G-CFI) will provide an Executive Secretary for the PSAB to administer operations of the board.

f. When an appeal is received Commandant (G-CFI) will:

(1) Govern the frequency of the meetings to review appeals;

(2) Set places and times of the meetings;

(3) Determine review procedures to be followed; and

(4) Handle all administrative matters.

g. The PSAB will adhere to the following procedures:

(1) Upon receipt of an appeal, the secretary will retrieve the investigations and/or other security files and notifies members of the PSAB.

(2) The PSAB will review the appeal correspondence and associated case files pursuant to the adjudication guidelines contained in chapter four of this Manual. The PSAB decision will be based solely on the written record including any writings submitted by the member. The member is entitled to a personal appearance before the PSAB to answer questions and submit any additional pertinent information. The member will be notified in writing by the board if during an initial meeting the board does not intend to overturn the Central Adjudication Facility (CAF) decision. The personal appearance will be arranged and funded by the individual's command.

(3) The President of the PSAB will sign and forward the final appeal decision to the appellant via his/her Commanding Officer with copies to the CAF. The appellant can appeal

the PSAB decision to the Department of Transportation Personnel Security Review Board (PSRB). Commandant (G-CFI) will retain the completed appeal file.

3. Reconsideration. Coast Guard military members whose security clearances or eligibility have been denied or revoked are not eligible for reconsideration by the PSAB for 1 year from the date of the CAF denial or revocation. Commanding Officers may request reconsideration by providing a CG-5588 request to the CAF via Commandant (G-CFI), together with their rationale as to why the denial or revocation should be reconsidered.

Q. Investigations Affecting Suitability for Coast Guard Service.

1. When a personnel security or suitability for service investigation reveals information that would affect a member's suitability for Coast Guard service, Commandant (G-CFI) will forward the investigation to Personnel Command for a final retention determination. If a favorable retention decision is made and a security clearance is required, the investigation will be returned to Commandant (G-CFI) to facilitate the security clearance determination.

2. The factors listed below may be considered as a basis for determining if a member is unsuitable for Coast Guard service:

   a. Misconduct or negligence in prior assignments that would have a bearing on efficient service, or would interfere with or prevent effective accomplishment of Coast Guard missions and responsibilities;

   b. Criminal conduct or dishonest conduct, which may have an impact on the members ability to perform his/her duties and responsibilities;

   c. Intentional false statement, deception, or fraud;

   d. Alcohol abuse of a nature and duration which suggests that the member would be prevented from performing his/her duties and responsibilities;

   e. Illegal use of narcotics, drugs, or other controlled substances, without evidence of substantial rehabilitation;

   f. Knowing and willful engagement in acts or activities designed to overthrow the U.S. Government by force; or,

g. Refusal to furnish testimony during an investigation, inquiry, or personnel security interview.

R. **Requests for Additional Information**. Commandant (G-CFI) and the central adjudication facility (CAF) are authorized to request additional pertinent information, forms or evaluation to resolve issues. Commanding Officers shall provide responses to those requests in a timely manner in order to expedite processing. Each request will contain a suspense date for response. The CAF shall be advised of any delays past that suspense date. Additional time to respond will be given when possible.

S. **Single Scope Background Investigations for Sensitive Compartmented Information**.

1. In order to grant access to Sensitive Compartmented Information (SCI), personnel are first required to possess a Top Secret clearance, granted by the Coast Guard Central Adjudication Facility (CAF). As such, a current SSBI is necessary. When required, personnel should follow the procedures previously described in this chapter in filling out the SF-86. Prior to actual submission of the forms, candidates for SCI access will be subject to a pre-nomination interview to determine their suitability for further processing for SCI access. The pre-nomination interview will be conducted by the Special Security Officer (SSO) if available or as directed by the cognizant security manager.

2. The CG-5588 will be filled out as previously noted with the following additions:

   a. Block 18: Check the box marked SCI and note authority (provided by the SSO).

   b. Block 20: Check the box marked SSBI, and

   c. Block 21: Check the Top Secret box and the SCI box.

3. To request SCI access for personnel who hold a current SSBI and Top Secret eligibility granted by the CAF, the SSO shall submit a CG-5588 and the completed pre-nomination interview to Commandant (G-OCI).

4. Any changes in personal status involving a current marriage, intention to or actual marriage to a foreign national, proposed name change, or changes in cohabitation shall be reported to the appropriate SSO. The member should provide the SSO an SF-86 on the spouse/cohabitant, (items 1-8, 13, member may sign for spouse). The SSO will prepare a CG-5588 and shall

annotate block 23 with "change in marital status/cohabitant status". The SSO will then forward a copy of the CG-5588 to Commandant G-O-CGIS.

T. **Administrative Withdrawal of Access**.

1. If an SSBI/PR is in progress at the time of the 5-year anniversary of the SSBI, the Top Secret clearance will not be administratively adjusted. However, if the Top Secret clearance is held based on a SSBI that is older than 5 years and the individual fails to provide paperwork for a periodic reinvestigation within 30 days, the Commanding Officer will remove access and notify the cognizant security manager.

2. When a Secret clearance is held based on an investigation that is older than 10 years and the individual fails to provide paperwork for a periodic reinvestigation within 30 days, the Commanding Officer will remove access and notify the cognizant security manager.

3. Commanding Officers will administratively withdraw an individual's access if the individual refuses to submit any required investigative paperwork.

4. A waiver to the above requirements maybe requested in writing from the cognizant Security Manager.

U. **Temporary Access**. Coast Guard military personnel may be granted temporary access if the individual has met the requirements for either an interim or final clearance, but does not currently hold a security clearance at that level. Temporary access to SCI material, although not typically justified, falls under the purview of Commandant (G-OCI). Situations in which temporary access may be justified include attendance at a classified meeting or training session, participation in advancement examinations or annual reserve active duty for training. If temporary access is justified, the Commanding Officer may, after favorable review of locally available records, allow access or certify to another command the individual's eligibility for access. This provision is made to relieve commands and the central adjudication facility (CAF) of the administrative burden of taking normal action to temporarily reissue or raise an individual's security clearance temporarily. It does not apply when an individual's assigned duties require continued access, even intermittently. Temporary access is limited to 30 days, and will be granted no more than twice per year to any one individual and may not be granted under any circumstances to individuals whose security clearance, eligibility or access has been denied or revoked. When access is granted, a CG-5588 will be completed citing this paragraph in the remarks section and will indicate the level of temporary access and the dates authorized. CG-5588's for temporary access will be maintained by the command for a period of four years after the temporary access is removed.

V. **Continuous Evaluation Program (CEP)**.

1. Derogatory Information.

   a. Each member's eligibility for access to classified information or assignment to sensitive duties shall be subject to the CEP. Commanding Officers shall report all derogatory information relevant to security on personnel holding a security clearance eligibility to Commandant (G-CFI) via CG-5588 with an information copy to the cognizant Security Manager, (information involving civil arrest or conviction will also be sent to Personnel Command (CGPC-OPM/EPM and ADM-3) as soon as the incident occurs. Coast Guard Special Agents shall report derogatory information to Commandant (G-CFI), upon discovery. The CG-5588 will cite the incident and the date it occurred, if access has been suspended and final disposition (if known). If the incident is pending a final disposition, the remarks section should be clearly marked "**INITIAL REPORT**". Documentation shall be attached as an enclosure on all reports. This applies to all personnel subject to the personnel security program. The remarks section of the CG-5588 will provide a brief summary of the specific unfavorable information. An additional sheet is authorized if space in the remarks section is insufficient.

   b. When an **initial report** is sent (depending on the severity of the derogatory information), Commandant (G-CFI) will hold any adjudicative action in abeyance for 60 days or until a **final report** is received. If the investigation, inquiry or disposition is still pending at the end of 60 days, forward a CG-5588 to Commandant (G-CFI) marked "**INTERIM REPORT**" and provide the progress. Interim reports shall be submitted every 60 days until the investigation, inquiry or disposition is finalized. The final results shall be forwarded to Commandant (G-CFI) via CG-5588 marked as "**FINAL REPORT**" in the remarks section.

   c. Derogatory information shall be reported to Commandant (G-CFI). Such information shall not be withheld based on the individual's work performance. Complete records of reported derogatory information are maintained at Commandant (G-CFI) and the Central Adjudication Facility (CAF) only. Therefore, a qualified determination can be made at the Commandant (G-CFI)/CAF level only. It is therefore essential that all derogatory information outlined in para (d) below received on personnel having a security clearance eligibility be reported immediately to Commandant (G-

CFI), including information discovered or obtained during the course of investigations of Coast Guard personnel.

d. Derogatory information which is found in the following personnel security factors will be immediately reported to Commandant (G-CFI) including any action taken by the command:

(1) Illegal use or abuse of drugs or alcohol

(2) Theft or dishonesty

(3) Lack of reliability, irresponsibility, immaturity, instability or recklessness.

(4) The use of force, violence or weapons or actions that indicate disregard for the law due to multiplicity of minor infractions.

(5) Moral turpitude, sexual promiscuity, aberrant, deviate or bizarre sexual conduct or behavior, transvestism, transsexualism, indecent exposure, rape, contributing to the delinquency of a minor, child molestation, spouse-swapping, window peeping and similar situations from whatever source.

(6) Records or testimony of military service where the individual was involved in serious offenses or incidents that would reflect adversely on the honesty, reliability, trustworthiness or stability of the individual.

(7) Mental, nervous, emotional psychological, psychiatric or character disorders/behavior or treatment reported or alleged from any source.

(8) Excessive indebtedness, bad checks, financial difficulties or irresponsibility, unexplained affluence, bankruptcy or evidence of living beyond the individual's means.

(9) Any other significant information relating to the criteria included in chapter four of this manual.

Note: All personnel are responsible for reporting known or discovered derogatory information to their chain of command and Commandant (G-CFI).

2. Repeated Minor Infractions. When the individual has clearance eligibility, repeated minor infractions or infractions serious enough to cause a

member to be processed under the Uniform Code of Military Justice (UCMJ), will be reported.

3. Relationship With Foreign National. Any Coast Guard military member who marries or cohabits with a foreign-born, non-U.S. citizen must inform his or her Commanding Officer, must complete an SF-86 on the spouse/cohabitant and must forward the form to Commandant (G-O-CGIS) within 30 days of the marriage/cohabitation. This must be done regardless of whether the military member is eligible for or possesses a security clearance. All members shall be cautioned that marriage or cohabitation with a foreign-born, non-U.S. citizen may result in the loss of eligibility for a security clearance. The requirements of this subsection are in addition to any other requirements of directives, publications, laws or regulations, which may apply.

W. **Suspension of Access**. When questionable or unfavorable information becomes available concerning an individual who has been granted access, the Commanding Officer may limit or suspend access. **Once access is suspended or limited, it can only be restored by a CAF determination or approval from Commandant (G-CFI).** Commands are encouraged to consult with their cognizant security manager prior to suspension or limitation of access. Once access is suspended or limited the cognizant Security Manager shall be notified immediately. The Commanding Officer shall forward **all pertinent information** concerning the individual to Commandant (G-CFI) for a clearance eligibility determination via CG form 5588 completing items 1 thru 8, 24 and 26 and note "**INITIA**L, **INTERIM** or **FINAL** l report of derogatory information" in block 22. **Permanent change of station orders which may already be in effect on the individual must be canceled or held in abeyance and proper notification made to Commander, CG Personnel Command.**

X. **Tracer Actions**. **Tracer actions will not be submitted if the member has been granted an interim clearance**. If an interim clearance cannot be granted, tracer requests may be sent to Commandant (G-CFI) via CG form 5588 completing items 1 thru 8 and 24 thru 26 noting "TRACER REQUEST, NACLC, SSBI OR SSBI-PR (as appropriate) SUBMITTED YYMMDD" in the remarks section.

Y. **Security Clearances and Access for non-United States Citizens**.

1. The authority to grant clearance or access to non-U.S. citizens has not been delegated to the Coast Guard. Every effort shall be made to ensure that non-U.S. citizens are not employed in duties that require access to classified information. However, when it is determined that employment of a non-U.S. citizen in duties requiring access to certain classified information relating to a specific program is necessary in furthering the mission of the Coast Guard or national security, and when such access is

clearly consistent with the interests of national security, a clearance or limited access authorization may be requested from the office of the Secretary via Commandant (G-CFI) in accordance with the procedures outlined below.

2. Non-immigrant aliens are not eligible for any level of security clearance, but may be processed for Limited Access Authorization when circumstances justify.

3. Immigrant Aliens

   a. When an immigrant alien requires access to classified material (Secret or confidential only) consideration should be given to requesting issuance of a Limited Access Authorization by letter to Commandant (G-CFI). If this is impracticable, the command proposing such access shall submit a letter request for processing of a security clearance to Commandant (G-CFI). Either request must explain the reasons why the clearance is needed, identify the specific duties that require access to classified information and the nature of the material to which access is required.

   b. The requesting command must ascertain that the individual has valid immigrant alien status and include a statement to that effect on the request. Such status may be determined by citing the Alien Registration Receipt card (INS Form I-151 or I-551), issued by the Immigration and Naturalization Service. Any member not having such a card must be considered as a non-immigrant alien.

      (1) The I-151 is a laminated, billfold sized blue or green card bearing the person's photograph, name, date of birth and alien registration number, and date and port of entry symbol.

      (2) The I-551 is a newer card of similar size that is laminated and bears the person's photograph, name, date of birth and alien registration number. The reverse of the card contains numerical data that is only decipherable by the USINS except for the alien registration number that appears in the block in the upper left and which should correspond to the number on the front of the card.

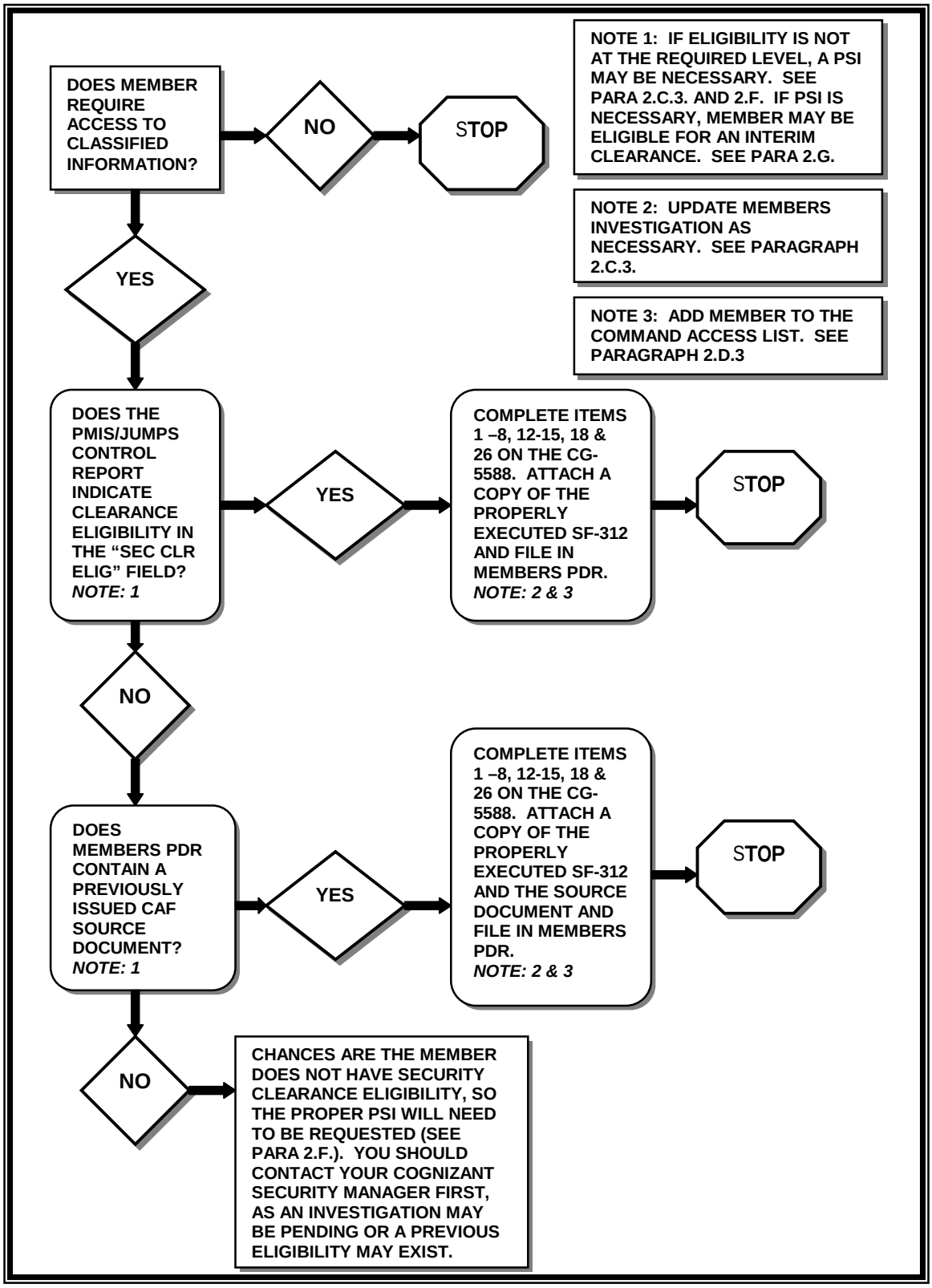
   c. The letter request shall be accompanied by a request for a SSBI, if such an investigation has not already been conducted on the individual.

d. Commandant (G-CFI) will review the letter request and forward it to the Office of the Secretary for consideration. The Director, Office of Security and Administrative Management (Office of the Secretary) may issue an Interim Secret or Confidential clearance to an immigrant alien based upon the completion of a favorable National Agency Check pending the completion of an SSBI. When the SSBI is completed, the Director has the discretion to issue the final clearance or, a Limited Access Authorization in lieu of a security clearance.

e. When an individual is admitted to the U.S. for permanent residence, a presumption is established that there has been a change of national allegiance from the native country to that of the U.S. When an individual becomes eligible for citizenship, but elects not to be a citizen, the presumption of primary national allegiance to the U.S. is placed in doubt. Accordingly, if an immigrant alien does not become a U.S. citizen within 12 months after becoming eligible for citizenship, any personnel security clearance shall be administratively reviewed to determine if it is clearly consistent with the national security to continue the clearance. Non-U.S. citizens currently holding clearances who are eligible for U.S. citizenship may continue to have the clearance for a period of 12 months after which their status will be reviewed to determine continuing need in accordance with this Manual.

f. When a security clearance or Limited Access Authorization is received, access may be granted as necessary.

g. Immigrant aliens will not be granted access to Top Secret material.


DOES MEMBER REQUIRE ACCESS TO CLASSIFIED INFORMATION?
NO
STOP
YES
NOTE 1: IF ELIGIBILITY IS NOT AT THE REQUIRED LEVEL, A PSI MAY BE NECESSARY. SEE PARA 2.C.3. AND 2.F. IF PSI IS NECESSARY, MEMBER MAY BE ELIGIBLE FOR AN INTERIM CLEARANCE. SEE PARA 2.G.
NOTE 2: UPDATE MEMBERS INVESTIGATION AS NECESSARY. SEE PARAGRAPH 2.C.3.
NOTE 3: ADD MEMBER TO THE COMMAND ACCESS LIST. SEE PARAGRAPH 2.D.3
DOES THE PMIS/JUMPS CONTROL REPORT INDICATE CLEARANCE ELIGIBILITY IN THE "SEC CLR ELIG" FIELD? NOTE: 1
YES
COMPLETE ITEMS 1 –8, 12-15, 18 & 26 ON THE CG-5588. ATTACH A COPY OF THE PROPERLY EXECUTED SF-312 AND FILE IN MEMBERS PDR. NOTE: 2 & 3
STOP
NO
DOES MEMBERS PDR CONTAIN A PREVIOUSLY ISSUED CAF SOURCE DOCUMENT? NOTE: 1
YES
COMPLETE ITEMS 1 –8, 12-15, 18 & 26 ON THE CG-5588. ATTACH A COPY OF THE PROPERLY EXECUTED SF-312 AND THE SOURCE DOCUMENT AND FILE IN MEMBERS PDR. NOTE: 2 & 3
STOP
NO
CHANCES ARE THE MEMBER DOES NOT HAVE SECURITY CLEARANCE ELIGIBILITY, SO THE PROPER PSI WILL NEED TO BE REQUESTED (SEE PARA 2.F.). YOU SHOULD CONTACT YOUR COGNIZANT SECURITY MANAGER FIRST, AS AN INVESTIGATION MAY BE PENDING OR A PREVIOUS ELIGIBILITY MAY EXIST.

DEPARTMENT OF TRANSPORTATION
U.S. COAST GUARD
CG-5588 (REV. 6/01)

PERSONNEL SECURITY ACTION

PART 1 – SUBJECT INFORMATION

(ITEMS 1 THROUGH 8 MUST BE COMPLETED FOR ALL ACTIONS)

1. Name (Last First Middle)	2. SSN	3. Pay Grade/Civ. Series & Grade	4. Rank/Rate (Military)

5. Status	6. Former Maiden Name/Aliases	7. Date of Birth (YYMMDD)	8. Place of Birth

Items 9 through 11 required only when requesting SCI eligibility determination

9. Date and Place of Current Marriage (YYMMDD)	10. Date and Place of Divorce (YYMMDD)

11. Citizenship of: a. Parents:_____ b. Brothers:_____ c. Sisters:_____
d. Spouse/Cohabitant:_____ e. Children: _____

PART II – LOCAL SECURITY REQUIREMENTS/CLEARANCE REAPPROVAL

12. U.S. Citizenship verified: Yes [] No [] By whom_____

13. Local Records Check Completed: (MIL) PDR[] HEALTH[] (CIV) OPF [] RESULTS: Favorable [] Unfavorable[] Conducted by:_____Date:_____

14. Subject has continuous service with no break greater than 24 months: Yes[] No []

15. Subject has a _____(type of investigation) Completed on (YYMMDD)_____ completed by _____

Clearance eligibility:_____ Method of verification: _____ Reapproved at (level)_____Reapproval signature:_____Date:_____

Date SF-312 executed(YYMMDD): _____

PART III – INTERIM CLEARANCE

16. Interim Top Secret granted(MIL ONLY) (YYMMDD)_____ Type of previous investigation and date: _____

SSBI paperwork submitted via District Security Manager to G-O-CGIS (YYMMDD)_____

17. (MIL & CIV) Interim Secret/Confidential (circle one) granted (YYMMDD)_____

NACLC paperwork submitted (YYMMDD): _____

Ensure items 12-14 are completed for interim clearance

PART IV – ACCESS INFORMATION

18. Subject granted access at (level): Top Secret [] Secret [] Confidential [] SCI [] Authority for SCI:_____

Date access granted (YYMMDD):_____Appropriate briefing conducted: Yes[] No[]

Date access terminated (YYMMDD) _____ Reason:_____

19. Suspended subjects access to all Classified information [] on (YYMMDD):_____

Reason for suspension:_____

PART V – ACTION REQUESTED

20. Investigation Requested: SSBI [] PR-SSBI [] NACLC [] NACLC UPDATE [] LI []

21. CAF determination requested: TOP SECRET [] SECRET [] CONFIDENTIAL [] SCI []

22. OTHER:_____23. Signature:_____Date:_____

PART VI – CAF ACTION

24. Investigation requested(YYMMDD)_____Investigation completed(YYMMDD) _____

Case Number_____Investigation received (YYMMDD)_____Clearance Authorized: _____

Authorized by:_____ Date (YYMMDD)_____

PART VII – ADMINISTRATIVE

27. Complete Mailing Address of Requester:	25. Remarks/Enclosures (include reason for investigation/clearance requested) 26.Military billet Control Number (BCN):_____Civilian position control number:_____ Security Manager/Command Security Officer Approval:_____ Date:_____ ***ITEM 25 REQUIRED FOR SSBI AND PR-SSBI REQUESTS***

DEPARTMENT OF TRANSPORTATION
U.S. COAST GUARD
CG-5588 (REV. 6/01)

PERSONNEL SECURITY ACTION

PART 1 – SUBJECT INFORMATION

(ITEMS 1 THROUGH 8 MUST BE COMPLETED FOR ALL ACTIONS)

1. Name (Last First Middle)	2. SSN	3. Pay Grade/Civ. Series & Grade	4. Rank/Rate (Military)

5. Status	6. Former Maiden Name/Aliases	7. Date of Birth (YYMMDD)	8. Place of Birth

Items 9 through 11 required only when requesting SCI eligibility determination

9. Date and Place of Current Marriage (YYMMDD)	10. Date and Place of Divorce (YYMMDD)

11. Citizenship of: a. Parents:_____ b. Brothers:_____ c. Sisters:_____
d. Spouse/Cohabitant:_____ e. Children: _____

PART II – LOCAL SECURITY REQUIREMENTS/CLEARANCE REAPPROVAL

12. U.S. Citizenship verified: Yes [] No [] By whom_____

13. Local Records Check Completed: (MIL) PDR[] HEALTH[] (CIV) OPF [] RESULTS: Favorable [] Unfavorable[] Conducted by:_____Date:_____

14. Subject has continuous service with no break greater than 24 months: Yes[] No []

15. Subject has a _____(type of investigation) Completed on (YYMMDD)_____ completed by _____

Clearance eligibility:_____ Method of verification: _____ Reapproved at (level)_____Reapproval signature:_____Date:_____

Date SF-312 executed(YYMMDD): _____

PART III – INTERIM CLEARANCE

16. Interim Top Secret granted(MIL ONLY) (YYMMDD)_____ Type of previous investigation and date: _____

SSBI paperwork submitted via District Security Manager to G-O-CGIS (YYMMDD)_____

17. (MIL & CIV) Interim Secret/Confidential (circle one) granted (YYMMDD)_____

NACLC paperwork submitted (YYMMDD): _____

Ensure items 12-14 are completed for interim clearance

PART IV – ACCESS INFORMATION

18. Subject granted access at (level): Top Secret [] Secret [] Confidential [] SCI [] Authority for SCI:_____

Date access granted (YYMMDD):_____Appropriate briefing conducted: Yes[] No[]

Date access terminated (YYMMDD) _____ Reason:_____

19. Suspended subjects access to all Classified information [] on (YYMMDD):_____

Reason for suspension:_____

PART V – ACTION REQUESTED

20. Investigation Requested: SSBI [] PR-SSBI [] NACLC [] NACLC UPDATE [] LI []

21. CAF determination requested: TOP SECRET [] SECRET [] CONFIDENTIAL [] SCI []

22. OTHER:_____23. Signature:_____Date:_____

PART VI – CAF ACTION

24. Investigation requested(YYMMDD)_____Investigation completed(YYMMDD) _____

Case Number_____Investigation received (YYMMDD)_____Clearance Authorized: _____

Authorized by:_____ Date (YYMMDD)_____

PART VII – ADMINISTRATIVE

27. Complete Mailing Address of Requester:	25. Remarks/Enclosures (include reason for investigation/clearance requested) 26.Military billet Control Number (BCN):_____Civilian position control number:_____ Security Manager/Command Security Officer Approval:_____ Date:_____ ***ITEM 25 REQUIRED FOR SSBI AND PR-SSBI REQUESTS***

CHAPTER THREE

SECURITY AWARENESS AND COUNTER-ESPIONAGE

A. Security Awareness.

1. Each Coast Guard member must be provided annual briefings in order to ensure that they understand his/her responsibility in regards to national security, and proper handling of classified and sensitive information.

2. The Security Awareness, Training and Education (SATE) Program, COMDTINST M5528.1 (series), contains example briefings which may be used to develop a briefing that will meet the specific needs of the command. An example of these and other briefings are also contained in enclosure (4) of this manual.

3. The Command Security Officer is responsible for ensuring security briefings are properly conducted and documented. The Command Security Officer may delegate other individuals to conduct the briefings; however, the ultimate responsibility rests with the Command Security Officer.

4. The briefings listed below represent the **minimum** requirements:

   a. Arrival Briefing. All personnel reporting aboard a Coast Guard unit will be given an arrival briefing. The briefing will make the individual aware of appropriate security personnel at the unit, their responsibilities and how to contact them. The briefing will also ensure that the individual is able to identify classified material and is knowledgeable of actions to be taken if classified material is discovered unattended. The briefing should identify any unit specific threats or concerns.

   b. Access Briefing. Personnel who have been determined to require access to classified information will be given an access briefing. This briefing will be conducted prior to actual access to any classified information. The briefing will ensure that the individual is aware of his/her responsibility in protecting classified information, unauthorized disclosure, and compromise reporting procedures.

   c. SF-312 Nondisclosure agreement.

      (1) All Coast Guard personnel who will be granted a clearance for access to classified information **must** be briefed and execute a SF-312 nondisclosure agreement.

(2) **This briefing and agreement need only be executed once in an individuals career provided it is executed correctly and certified copies are locally available or a SF 312 signature date in the CGHRMS database.**

(3) Commanding Officers will ensure personnel receive the briefing required in the terms of the SF 312 and have the opportunity to read the sections of titles 18 and 50 of the United States Code and other acts referred to in the agreement.

(4) Subsequent to its execution, the SF-312 must be accepted on behalf of the United States. The accepting official can be the Commanding Officer, the Executive Officer or the Command Security Officer.

(5) If an individual refuses to sign a SF 312, the command will deny him/her access to classified information, terminate any current access immediately and inform Commandant (G-CFI) via CG-5588 with a copy to the cognizant security manager.

(6) Original SF-312's will be sent to Personnel Command (CGPC-ADM-3) with copies in the members PDR. Personnel Command (CGPC-ADM-3) will retain SF-312's as part of the member's permanent record. Improperly executed SF-312's will be returned to the unit with a copy to the cognizant Security Manager.

d. Foreign Travel Briefing. All personnel traveling to a foreign country must be given a foreign travel briefing whether the travel is official or in a leave situation. The briefing will inform personnel of general safety precautions and any information specific to the country being visited. After the travel is conducted, a Counter-Espionage debrief will be conducted by the Command Security Officer (CSO) to provide individual(s) the opportunity to report any incident - no matter how insignificant it might have seemed, that could have security implications. Any suspicious incidents shall be reported to the cognizant Security Manager in accordance with the provisions of this chapter.

e. Refresher Briefings. Once a year, all personnel who have access to classified information will receive a refresher briefing. Refresher briefings will be conducted by direction of the Command Security Officer but may be given by supervisory personnel. Refresher briefings are designed to enhance security awareness and may be given to all assigned personnel in the form of a command security stand down. The refresher brief should touch on general security matters and any recent changes in policies or procedures.

f. Final Termination Briefing. Personnel shall be given a termination briefing upon termination of government service, or when a clearance is revoked for cause. The briefing shall remind personnel to return all classified material in

their possession, and they remain subject to the provisions of the criminal code and other applicable laws relating to the unauthorized disclosure of classified information. The SF-312 will be utilized to conduct this briefing and sent to Personnel Command (CGPC-ADM-3) for inclusion in the member's permanent record.

B. Documentation of Briefings.

1. Commands will develop their own briefings based on the minimum requirements above. A record of individuals briefed will be attached and maintained for a period of four years after the latest action. The record will contain names of individuals receiving and conducting the brief, the date conducted and signatures of both. If unit level briefings are conducted a roster may be attached rather than individual entries. Each new briefing must have its own record in order to ensure that there is documentation not only of who was briefed, but what the brief consisted of. Whenever a brief is changed or altered, a new record of briefing is required.

C. Counter-Espionage.

1. General.

   a. The Coast Guard Counter-Espionage Program is a process associated with the detection and reporting of possible espionage and other security related activities, which if left undetected, could cause grave damage to national security, the interest of the Coast Guard, and the personnel assigned to the Coast Guard. This element of the overall Security Program plays an important role in the protection of classified and sensitive information, and the protection of individuals against subversion and terrorism, and the protection of facilities, ships, aircraft and other resources or material against sabotage and terrorism.

   b. In the performance of its missions the Coast Guard interacts with other countries in the areas of law enforcement, military exchanges and port visits. This interaction may subject Coast Guard personnel to foreign intelligence collection efforts. These hostile intelligence efforts may continue regardless of shifts in governments and policies of states.

   c. All Coast Guard personnel, whether they have access to classified information or not, shall report to their CSO any activities described in this chapter involving themselves or others. Commanding Officers will, in turn, notify the cognizant Security Manager in accordance with the procedures set forth in this chapter.

d. Coast Guard personnel who have access to classified or sensitive information shall be aware of the techniques employed by foreign and domestic hostile intelligence personnel, in attempting to obtain classified and or sensitive information and their responsibility for reporting such attempts.

2. Sabotage Espionage or Deliberate Compromise.

   a. Individuals becoming aware of possible acts of sabotage, espionage, deliberate compromise or other subversive activities shall report all available information concerning such action immediately to their CSO. The Command receiving the report shall notify the cognizant Security Manager. If the cognizant Security Manager cannot be contacted immediately and the report concerns sabotage, indicates that there is a serious threat to the security of classified information through espionage, or immediate flight or defection of an individual, the unit shall send an immediate message classified at the level of the threatened information action to Commandant (G-CFI) with an information copy to the cognizant Security Manager.

   b. The cognizant Security Manager shall be notified immediately of any requests, through other than official channels, for classified national security information from anyone regardless of nationality, or for unclassified information from any individual believed to be in contact with a foreign intelligence service. Examples of requests to be reported include attempts to obtain: names, duties, personal data or characterizations of Coast Guard personnel; technical orders, manuals, regulations, base directories, personnel rosters or unit manning tables; and information about the designation, strength, mission, combat posture, and development of ships, aircraft and weapons systems.

   c. The Security Manager will advise the unit of what additional action, if any will be taken. The Security Manager will then notify Commandant (G-CFI) who will effect liaison and coordination with pertinent members of the U.S. security countermeasures community, the Coast Guard Office of Intelligence (Commandant (G-OCI)) and the Coast Guard Investigative Service (Commandant (G-O-CGIS)).

3. Suicides or Attempted Suicides. When an individual with access to classified information commits or attempts to commit suicide, immediately report all available information to the cognizant Security Manager with an information copy to Commandant (G-CFI). The report should set forth the nature and extent of classified material to which the individual had access and the circumstances surrounding the incident. Classified material signed out to the individual will be immediately inventoried and accountability records reconciled. Combinations to all classified containers to which the person had access will be changed immediately. Discrepancies in classified holdings will be immediately reported as

a possible compromise per the Classified Information Management Program, COMDTINST M5510.23 (series).

4. Unauthorized Absence. When an individual (Military or Civilian) who has had access to classified material is absent without leave (AWOL), the individual's Commanding officer will attempt to determine if there are any indications that the person may place or attempt to place themselves under the control of a foreign nation or that their activities, behavior or associations may threaten national security. In those cases where there are such indications, the Commanding Officer shall immediately forward all available information to the cognizant Security Manager with an information copy to Commandant (G-CFI).

CHAPTER FOUR

ADJUDICATIVE GUIDELINES

A. PURPOSE. The following adjudicative guidelines were established pursuant to Executive Order 12968 and were approved by the President March 24, 1997. Access to Classified Information, for all U.S. government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information. They apply to persons being considered for initial or continued eligibility for access to classified information, or assignment to sensitive duties, to include sensitive compartmented information (SCI) and special access programs (SAP), and are to be used by government departments and agencies in all final clearance determinations.

B. ADJUDICATIVE PROCESS.

1. The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is an acceptable security risk. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines. The adjudication process is the careful weighing of a number of variables known as the whole person concept. All available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination. In evaluating the relevance of an individual's conduct, the adjudicator should consider the following factors:

    a. The nature, extent, and seriousness of the conduct
    b. The circumstances surrounding the conduct, to include knowledgeable participation
    c. The frequency and recency of the conduct
    d. The individual's age and maturity at the time of the conduct
    e. The voluntariness of participation
    f. The presence or absence of rehabilitation and other pertinent behavioral changes
    g. The motivation for the conduct
    h. The potential for pressure, coercion, exploitation, or duress
    i. The likelihood of continuation or recurrence

2. Each case must be judged on its own merits and final determination remains the responsibility of the specific department or agency. Any doubt concerning personnel being considered for access to classified information will be resolved in favor of the national security and considered final.

3. The ultimate determination of whether the granting or continuing of eligibility for a security clearance is clearly consistent with the interests of national security must be an overall common sense determination based upon careful consideration of the following, each of which is to be evaluated in the context of the whole person, as explained further below:

    a. Allegiance to the United States
    b. Foreign influence
    c. Foreign preference
    d. Sexual behavior
    e. Personal conduct
    f. Financial considerations
    g. Alcohol consumption
    h. Drug involvement
    i. Emotional, mental, and personality disorders
    j. Criminal conduct
    k. Security violations
    l. Outside activities
    m. Misuse of Information Technology Systems

4. Although adverse information concerning a single criterion may not be sufficient for an unfavorable determination, the individual may be disqualified if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or emotionally unstable behavior. Notwithstanding, the whole person concept, pursuit of further investigation may be terminated by an appropriate adjudicative agency in the face of reliable, significant, disqualifying, adverse information.

5. When information of security concern becomes known about an individual who is currently eligible for access to classified information, the adjudicator should consider whether the person:

    a. Voluntarily reported the information:
    b. Was truthful and complete in responding to questions
    c. Sought assistance and followed professional guidance, where appropriate;
    d. Resolved or appears likely to favorably resolve the security concern;
    e. Has demonstrated positive changes in behavior and employment;
    f. Should have his or her access temporarily suspended pending final adjudication of the information.

6. If after evaluating information of a security concern, the adjudicator decides that the information is not serious enough to warrant a recommendation of disapproval or revocation of the security clearance, it may be appropriate to recommend

approval with a warning that future incidents of a similar nature may result in revocation of access.

7. The information in bold print at the beginning of each adjudicative guideline provides a brief explanation of its relevance in determining whether it is clearly consistent with the interest of national security to grant or continue a person's eligibility for access to classified information.

C. ALCOHOL CONSUMPTION.

1. Excessive alcohol consumption often leads to the exercise of questionable judgment, unreliability, failure to control impulses, and increases the risk of unauthorized disclosure of classified information due to carelessness.

2. Conditions that could raise a security concern and may be disqualifying include:

    a. alcohol-related incidents away from work, such as driving while under the influence, fighting, child or spouse abuse, or other criminal incidents related to alcohol use;
    b. Alcohol-related incidents at work, such as reporting for work or duty in an intoxicated or impaired condition, or drinking on the job;
    c. Diagnosis by a credentialed medical professional of alcohol abuse or alcohol dependence;
    d. Habitual or binge consumption of alcohol to the point of impaired judgment;
    e. Consumption of alcohol, subsequent to a diagnosis of alcoholism by a credentialed medical professional and following completion of an alcohol rehabilitation program

3. Conditions that could mitigate security concerns include:

    a. The alcohol related incidents do not indicate a pattern;
    b. The problem occurred a number of years ago and there is no indication of a recent problem;
    c. Positive changes in behavior supportive of sobriety;
    d. Following diagnosis of alcohol abuse or alcohol dependence, the individual has successfully completed inpatient or outpatient rehabilitation along with aftercare requirements, participates frequently in meetings of Alcoholics Anonymous or a similar organization, abstained from alcohol for a period of at least 12 months, and received a favorable prognosis by a credentialed medical professional.

D. ALLEGIANCE TO THE UNITED STATES.

1. An individual must be of unquestioned allegiance to the United States. The willingness to safeguard classified information is in doubt if there is any reason to suspect an individual's allegiance to the United States.

2. Conditions that could raise a security concern and may be disqualifying include:

   a. Involvement in any act of sabotage, espionage, treason, terrorism, sedition, or other act whose aim is to overthrow the Government of the United States or alter the form of government by unconstitutional means;
   b. Association or sympathy with persons who are attempting to commit, or who are committing, any of the above acts;
   c. Association or sympathy with persons or organizations that advocate the overthrow of the United States Government, or any state or subdivision, by force or violence or by other unconstitutional means;
   d. Involvement in activities which unlawfully advocate or practice the commission of acts of force or violence to prevent others from exercising their rights under the Constitution or laws of the United States or of any state.

3. Conditions that could mitigate security concerns include:

   a. The individual was unaware of the unlawful aims of the individual or organization and severed ties upon learning of these;
   b. The individual's involvement was only with the lawful or humanitarian aspects of such an organization;
   c. Involvement in the above activities occurred for only a short period of time and was attributable to curiosity or academic interest;
   d. The person has had no recent proscribed involvement or association with such activities.

E. CRIMINAL CONDUCT.

1. A history or pattern of criminal activity creates doubt about a person's judgment, reliability and trustworthiness.

2. Conditions that could raise a security concern and may be disqualifying include:

   a. Any criminal conduct, regardless of whether the person was formally charged;
   b. A single serious crime or multiple lesser offenses

3. Conditions that could mitigate security concerns include

   a. The criminal behavior was not recent;
   b. The crime was an isolated incident;

c. The person was pressured or coerced into committing the act and those pressures are no longer present in that person's life;
d. The person did not voluntarily commit the act and/or the factors leading to the violation are not likely to recur;
e. There is clear evidence of successful rehabilitation.

F. DRUG INVOLVEMENT.

1. Improper or illegal involvement with drugs raises questions regarding an individual's willingness or ability to protect classified information. Drug abuse or dependence may impair social or occupational functioning, increasing the risk of an unauthorized disclosure of classified information.

2. Drugs are defined as mood and behavior altering:

   a. Drugs, materials, and other chemical compounds identified and listed in the Controlled Substances Act of 1970, as amended (e.g., marijuana or cannabis, depressants, narcotics, stimulants, and hallucinogens) and
   b. Inhalants and other similar substances.
   c. Drug abuse is the illegal use of a drug or use of a legal drug in a manner that deviates from approved medical direction.

3. Conditions that could raise a security concern and may be disqualifying include:

   a. Any drug abuse (see above definition);
   b. Illegal drug possession, including cultivation, processing, manufacture, purchase, sale, or distribution;
   c. Failure to successfully complete a drug treatment program prescribed by a credentialed medical professional.
   d. Current drug involvement, especially following the granting of a security clearance, or an expressed intent not to discontinue use, will normally result in an unfavorable determination.

4. Conditions that could mitigate security concerns include:

   a. The drug involvement was not recent;
   b. The drug involvement was an isolated or infrequent event;
   c. A demonstrated intent not to abuse any drugs in the future;
   d. Satisfactory completion of a drug treatment program prescribed by a credentialed medical professional.

G. EMOTIONAL, MENTAL AND PERSONALITY DISORDERS.

1. Emotional, mental, and personality disorders can cause a significant deficit in an individual's psychological, social and occupational functioning. These disorders are of security concern because they may indicate a defect in judgment, reliability or stability.

2. When appropriate, a credentialed mental health professional, acceptable to or approved by the government should be consulted so that potentially disqualifying and mitigating information may be fully and properly evaluated.

3. Conditions that could raise a security concern and may be disqualifying include:

    a. A diagnosis by a credentialed mental health professional that the individual has a disorder that could result in a defect in psychological, social, or occupational functioning;
    b. Information that suggests that an individual has failed to follow appropriate medical advice relating to treatment of a diagnosed disorder, e.g. failure to take prescribed medication;
    c. A pattern of high-risk, irresponsible, aggressive, anti-social or emotionally unstable behavior;
    d. Information that suggests that the individual's current behavior indicates a defect in his or her judgment or reliability.

4. Conditions that could mitigate security concerns include:

    a. There is no indication of a current problem;
    b. Recent diagnosis by a credentialed mental health professional that an individual's previous emotional, mental, or personality disorder is cured or in remission and has a low probability of recurrence or exacerbation;
    c. The past emotional instability was a temporary condition (e.g., one caused by a death, illness, or marital breakup), the situation has been resolved, and the individual is no longer emotionally unstable.

H. FINANCIAL CONSIDERATIONS.

1. An individual who is financially overextended is at risk of having to engage in illegal acts to generate funds. Unexplained affluence is often linked to proceeds from financially profitable criminal acts.

2. Conditions that could raise a security concern and may be disqualifying include:

    a. A history of not meeting financial obligations;

b. Deceptive or illegal financial practices such as embezzlement, employee theft, check fraud, income tax evasion, expense account fraud, filing deceptive loan statements, and other intentional financial breaches of trust;
c. Inability or unwillingness to satisfy debts;
d. Unexplained affluence;
e. Financial problems that are linked to gambling, drug abuse, alcoholism, or other issues of security concern.

3. Conditions that could mitigate security concerns include:

a. The behavior was not recent;
b. It was an isolated incident;
c. The conditions that resulted in the behavior were largely beyond the person's control (e.g., loss of employment, a business downturn, unexpected medical emergency, or a death, divorce or separation);
d. The person has received or is receiving counseling for the problem and there are clear indications that the problem is being resolved or is under control;
e. The affluence resulted from a legal source; and
f. The individual initiated a good-faith effort to repay overdue creditors or otherwise resolve debts.

I. FOREIGN INFLUENCE.

1. A security risk may exist when an individual's immediate family, including cohabitants, and other persons to whom he or she may be bound by affection, influence, or obligation are:

a. Not citizens of the United States or
b. May be subject to duress.

2. These situations could create the potential for foreign influence that could result in the compromise of classified information. Contacts with citizens of other countries or financial interests in other countries are also relevant to security determinations if they make an individual potentially vulnerable to coercion, exploitation, or pressure.

3. Conditions that could raise a security concern and may be disqualifying include:

a. An immediate family member, or a person to whom the individual has close ties of affection or obligation, is a citizen of, or resident or present in, a foreign country;
b. Sharing living quarters with a person or persons, regardless of their citizenship status, if the potential for adverse foreign influence or duress exists;
c. Relatives, cohabitants, or associates who are connected with any foreign government;

d. Failing to report, where required, associations with foreign nationals;
e. Unauthorized association with a suspected or known collaborator or employee of a foreign intelligence service;
f. Conduct which may make the individual vulnerable to coercion, exploitation, or pressure by a foreign government;
g. Indications that representatives or nationals from a foreign country are acting to increase the vulnerability of the individual to possible future exploitation, coercion or pressure;
h. A substantial financial interest in a country, or in any foreign owned or operated business that could make the individual vulnerable to foreign influence.

4. Conditions that could mitigate security concerns include:

a. A determination that the immediate family member(s), cohabitant, or associate(s) in question would not constitute an unacceptable security risk;
b. Contacts with foreign citizens are the result of official U.S. Government business;
c. Contact and correspondence with foreign citizens are casual and infrequent;
d. The individual has promptly reported to proper authorities all contacts, requests, or threats from persons or organizations from a foreign country, as required;
e. Foreign financial interests are minimal and not sufficient to affect the individual's security responsibilities.

J. FOREIGN PREFERENCE.

1. When an individual acts in such a way as to indicate a preference for a foreign country over the United States, then he or she may be prone to provide information or make decisions that are harmful to the interests of the United States.

2. Conditions that could raise a security concern and may be disqualifying include:

a. The exercise of dual citizenship;
b. Possession and/or use of a foreign passport;
c. Military service or a willingness to bear arms for a foreign country;
d. Accepting educational, medical, or other benefits, such as retirement and social welfare, from a foreign country;
e. Residence in a foreign country to meet citizenship requirements;
f. Using foreign citizenship to protect financial or business interests in another country;
g. Seeking or holding political office in the foreign country;
h. Voting in foreign elections; and

i. Performing or attempting to perform duties, or otherwise acting, so as to serve the interests of another government in preference to the interests of the United States.

3. Conditions that could mitigate security concerns include:

a. Dual citizenship is based solely on parents' citizenship or birth in a foreign country;
b. Indicators of possible foreign preference (e.g., foreign military service) occurred before obtaining United States citizenship;
c. Activity is sanctioned by the United States;
d. Individual has expressed a willingness to renounce dual citizenship.

K. MISUSE OF INFORMATION TECHNOLOGY SYSTEMS.

1. Noncompliance with rules, procedures, guidelines or regulations pertaining to information technology systems may raise security concerns about an individual's trustworthiness, willingness, and ability to properly protect classified systems, networks, and information.

2. Information Technology Systems include all related equipment used for the communication, transmission, processing, manipulation, and storage of classified or sensitive information.

3. Conditions that could raise a security concern and may be disqualifying include:

a. Illegal or unauthorized entry into any information technology system;
b. Illegal or unauthorized modification, destruction, manipulation, or denial of access to information residing on an information technology system;
c. Removal (or use) of hardware, software or media from any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations;
d. Introduction of hardware, software or media into any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines or regulations;

4. Conditions that could mitigate security concerns include:

a. The misuse was not recent or significant;
b. The conduct was unintentional or inadvertent;
c. The introduction or removal of media was authorized;
d. The misuse was an isolated event;
e. The misuse was followed immediately by a prompt, good faith effort to correct the situation.

L. OUTSIDE ACTIVITIES.

1. Involvement in certain types of outside employment or activities is of security concern if it poses a conflict with an individual's security responsibilities and could create an increased risk of unauthorized disclosure of classified information.

2. Conditions that could raise a security concern and may be disqualifying include:

    a. Any service, whether compensated, volunteer, or employment with:

        (1) A foreign country;
        (2) Any foreign national;
        (3) A representative of any foreign interest;
        (4) Any foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, foreign affairs, or protected technology.

3. Conditions that could mitigate security concerns include:

    a. Evaluation of the outside employment or activity indicates that it does not pose a conflict with an individual's security responsibilities;

    b. The individual terminates the employment or discontinues the activity upon being notified that it is in conflict with his or her security responsibilities.

M. PERSONAL CONDUCT.

1. Conduct involving questionable judgment, untrustworthiness, unreliability, or unwillingness to comply with rules and regulations could indicate that the person may not properly safeguard classified information.

2. The following will normally result in an unfavorable clearance action or administrative termination of further processing for clearance eligibility:

    a. Refusal to undergo or cooperate with required security processing, including medical and psychological testing; or

    b. Refusal to complete required security forms, releases, or provides full, frank and truthful answers to lawful questions of investigators, security officials or other official representatives in connection with personnel security or trustworthiness determination.

3. Conditions that could raise a security concern and may be disqualifying also include:

    a. Reliable, unfavorable information provided by associates, employers, coworkers, neighbors, and other acquaintances;
    b. The deliberate omission, concealment, or falsification of relevant and material facts from any personnel security questionnaire, personal history statement, or similar form used to conduct investigations, determine employment qualifications, award benefits or status, determine security clearance eligibility or trustworthiness, or award fiduciary responsibilities;
    c. Deliberately providing false or misleading information concerning relevant and material matters to an investigator, security official, competent medical authority, or other official representative in connection with a personnel security or trustworthiness determination;
    d. Personal conduct or concealment of information that increases an individual's vulnerability to coercion, exploitation or pressure;
    e. A pattern of dishonesty or rule violations;
    f. Association with persons involved in criminal activity.

4. Conditions that could mitigate security concerns include:

    a. The information was unsubstantiated or not pertinent to a determination of judgment, trustworthiness, or reliability;
    b. The falsification was an isolated incident, was not recent, and the individual has subsequently provided correct information voluntarily;
    c. The individual made prompt, good-faith efforts to correct the falsification before being confronted with the facts;
    d. Omission of material facts was caused or significantly contributed to by improper or inadequate advice of authorized personnel, and the previously omitted information was promptly and fully provided;
    e. The individual has taken positive steps to significantly reduce or eliminate vulnerability to coercion, exploitation, or pressure;
    f. A refusal to cooperate was based on advice from legal counsel or other officials that the individual was not required to comply with security processing requirements and, upon being made aware of the requirement, fully and truthfully provided the requested information;
    g. Association with persons involved in criminal activities has ceased.

N. SECURITY VIOLATIONS.

1. Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information.

2. Conditions that could raise a security concern and may be disqualifying include:

a. Unauthorized disclosure of classified information;
b. Violations that are deliberate or multiple or due to negligence.

3. Conditions that could mitigate security concerns include actions that:

a. Were inadvertent;
b. Were isolated or infrequent;
c. Were due to improper or inadequate training;
d. Demonstrate a positive attitude towards the discharge of security responsibilities.

O. SEXUAL BEHAVIOR.

1. Sexual behavior is a security concern if it involves a criminal offense, indicates a personality or emotional disorder, subjects the individual to undue influence or coercion, or reflects lack of judgment or discretion. (Sexual orientation or preference may not be used as a basis for or a disqualifying factor in determining a person's eligibility for a security clearance)

2. Conditions that could raise a security concern and may be disqualifying include:

a. Sexual behavior of a criminal nature, whether or not the individual has been prosecuted;
b. Compulsive or addictive sexual behavior when the person is unable to stop a pattern of self-destructive or high-risk behavior or that which is symptomatic of a personality disorder;
c. Sexual behavior that causes an individual to be vulnerable to undue influence or coercion;
d. Sexual behavior of a public nature and/or that which reflects lack of discretion or judgment.

3. Conditions that could mitigate security concerns include:

a. The behavior occurred during or prior to adolescence and there is no evidence of subsequent conduct of a similar nature;
b. The behavior was not recent and there is no evidence of subsequent conduct of a similar nature;
c. There is no other evidence of questionable judgment, irresponsibility, or emotional instability;
d. The behavior no longer serves as a basis for undue influence or coercion.

CHAPTER FIVE

DEPARTMENT OF ENERGY NUCLEAR SECURITY PROGRAM "Q" CLEARANCES

A. **General**. There are only a few positions/billets within the Coast Guard that are authorized access to Department of Energy (DOE) Restricted Data (Class Q) in connection with official duties. DOE Restricted Data relates to the design, manufacture and utilization of atomic/nuclear weapons; the production of special nuclear material or the use of nuclear material in the production of energy. DOE Restricted Data is assigned classification levels of Confidential, Secret or Top Secret, in keeping with the classification levels of other national defense information under provisions of E.O. 12958, National Security Information. Access to DOE Restricted Data is issued by the Department of Energy in accordance with the Atomic Energy Act of 1954 (Public Law 703, 83rd Congress).

B. **Responsibility.** Commandant (G-CFI), serving as the Director of Coast Guard Security, manages the Coast Guard portion of the DOE Nuclear Security (Class Q) clearance program, and is the final determining authority within the Coast Guard regarding the issuance of DOE clearances for Coast Guard personnel.

C. **Submission of Request for DOE Clearances.** Commands may obtain required forms and guidance from Commandant (G-CFI). Upon completion of the required forms by a military member or civilian employee of the Coast Guard requiring a DOE "Q" clearance, the command shall submit a written request, with sufficient justification, and the completed forms to Commandant (G-CFI). Upon adjudication and approval, G-CFI will forward the commands request to DOE for final DOE approval and issuance of a "Q" clearance. The following forms and information shall be submitted:

1. SF 86, Questionnaire for Sensitive Positions, original and 2 copies;

2. DOE F 5631.18 Security Acknowledgment Statement;

3. SF 87, Fingerprint Chart, 2 originals;

4. Information regarding any background investigations or derogatory information that the requesting command may have in its files regarding the individual.

D. **Unfavorable Cases.** Decisions by the Director of Coast Guard Security (G-CFI) or DOE to grant or to deny Restricted Data Clearance or Access, are not subject to review or appeal by Coast Guard civilian employees or military members. Information obtained during the DOE clearance/access process may be utilized to make other security and suitability for employment determinations, as outlined in this manual.

E. **Notification of Clearance.** Commandant (G-CFI) will notify the civilian employee or military member, via his/her command, of the issuance of a DOE Restricted Data Clearance. Commandant (G-CFI) will maintain the source document for the notification.

F. **Access Briefing.** The Command Security Officer or Command Classified Material Control Officer of the requesting Command will be responsible for providing a Q Clearance Security Briefing, through the utilization of briefing material provided by Commandant (G-CFI). The briefing official shall ensure that the person is thoroughly familiar with procedures required for safeguarding classified information and the special requirements relating to access to DOE Restricted Data. The briefing official shall also execute DOE Form 563 1. 18, Acknowledgment Statement, and return the form to Commandant (G-CFI), 2100 Second Street SW, Washington, DC 20593.

G. **Termination of Clearance.** Commands shall notify Commandant (G-CFI) when a DOE clearance/access is no longer required by the civilian employee or military member, because of duty changes, transfer or termination from employment or for any other reason. The employee or military member will be appropriately debriefed by the Command Security Officer or Classified Material Control Officer, who shall execute DOE Form F 5631.29, DOE Security Termination Statement, in duplicate. The Command will forward the DOE Security Termination Statement to Commandant (G-CFI), who will notify the Department of Energy that access is no longer required and request termination of the clearance. Commandant (G-CFI) will forward one copy of DOE Form F 5631.29 signed by the individual to DOE, and one shall be retained by Commandant (G-CFI).

H. **Transfer of Clearance.** If an employee or military member transfers to the Coast Guard from another DOT administrations or from another Federal agency, and prior to the transfer was issued a DOE Q clearance and access to DOE Restricted Data, the command may request that the Q clearance and access authorization be transferred with the employee or military member to the Coast Guard. The command shall send their request to Commandant (G-CFI), with name, social security number, and the DOE case file number (example: WA-123456), who will make a final determination for the Coast Guard, and if favorable, forward the request to DOE.

Investigative Standards for Background Investigations for Access to Classified Information

1. ***Introduction***. The following investigative standards are established for all United States Government Civilian and Military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information, to include Sensitive Compartmented Information and Special Access Programs, and are to be used by government departments and agencies as the investigative basis for final clearance determinations. However, nothing in these standards prohibits an agency from using any lawful investigative procedures in addition to these requirements in order to resolve any issue identified in the course of a background investigation or reinvestigation.

2. ***The Three Standards***. There are three standards (Table 1 in the Appendix summarizes when to use each one):

(a) The investigation and reinvestigation standards for "L" access authorizations and for access to CONFIDENTIAL and SECRET (including all SECRET-level Special Access Programs not specifically approved for enhanced investigative requirements by an official authorized to establish Special Access Programs by sect. 4.4 of Executive Order 12958);

(b) The investigation standard for "Q" access authorizations and for access to TOP SECRET (including TOP SECRET Special Access Programs) and Sensitive Compartmented Information; and

(c) The reinvestigation standard for continued access to the levels listed in para. 2(b).

3. ***Exception to Periods of Coverage***. Some elements of standards specify a period of coverage (e.g., seven years). Where appropriate, such coverage may be shortened to the period from the subject's eighteenth birthday to the present or to two years, which is longer.

4. ***Expanding Investigations***. Investigations and reinvestigations may be expanded under the provisions of Executive Order 12968 and other applicable statutes and Executive Orders.

5. ***Transferability***. Investigations that satisfy the requirements of a given standard and are current meet the investigative requirements for all levels specified for the standard. They shall be mutually and reciprocally accepted by all agencies.

6. ***Breaks in Service***. If a person who requires access has been retired or separated from US government employment for less than two years and is the subject of an investigation that is otherwise current, the agency regranting the access will, as a minimum, review an updated Standard Form 86 and applicable records. A reinvestigation is not required unless the review indicates the person may no longer satisfy the standards of Executive Order 12968 (see Table 2).

7. ***The National Agency Check***. The National Agency Check is a part of all investigations and reinvestigations. It consists of a review of:

(a) Investigative and criminal history files of the FBI, including a technical fingerprint search;

(b) OPM's Security/Suitability Investigations Index; and

(c) DoD's Defense Clearance and Investigations Index; and

(d) Such other national agencies (e.g., CIA, INS) as appropriate to the individual's background.

STANDARD A

National Agency Check with Local Agency Checks and

Credit Check (NACLC)

8. ***Applicability.*** Standard A applies to investigations and reinvestigations for:

(a) *Access to CONFIDENTIAL and SECRET* (including all SECRET-level Special Access Programs not specifically approved for enhanced investigative requirements by an official authorized to establish Special Access Programs by sect. 4.4 of Executive Order 12958), and

(b) "L" access authorizations.

9. ***For Reinvestigations.*** When to Reinvestigate. The reinvestigation may be initiated at any time following completion of, but not later than ten years (fifteen years for CONFIDENTIAL) from the date of, the previous investigation or reinvestigation. (Table 2 reflects the specific requirements for when to request a reinvestigation including when there has been a break in service.)

10. ***Investigative Requirements***. Investigative requirements are as follows:

(a) *Completion of Forms*: Completion of Standard Form 86, including applicable releases and supporting documentation.

(b) *National Agency Check*: Completion of a National Agency Check.

(c) *Financial Review*: Verification of the subject's financial status, including credit bureau checks covering all locations where the subject has resided, been employed, or attended school for six months or more for the past seven years.

(d) *Date and Place of Birth*: Corroboration of date and place of birth through a check of appropriate documentation, if not completed in any previous investigation; a check of Bureau of Vital Statistics records when any discrepancy is found to exist.

(e) *Local Agency Checks*: As a minimum, all investigations will include checks of law enforcement agencies having jurisdiction where the subject has lived, worked, and/or attended school within the last five years, and, if applicable, of the appropriate agency for any identified arrests.

11. ***Expanding the Investigation***. The investigation may be expanded if necessary to determine if access is clearly consistent with the national security.

STANDARD B

Single Scope Background Investigation (SSBI)

12. ***Applicability***. Standard B applies to initial investigations for:

(a) *Access to TOP SECRET* (including TOP SECRET Special Access Programs) and Sensitive Compartmented Information; and

(b) *"Q" access authorizations*.

13. ***Investigative Requirements***. Investigative requirements are as follows:

(a) *Completion of Forms*: Completion of Standard Form 86, including applicable releases and supporting documentation.

(b) *National Agency Check*: Completion of a National Agency Check.

(c) *National Agency Check for the Spouse or Cohabitant* (if applicable): Completion of a National Agency Check, without fingerprint cards, for the spouse or cohabitant.

(d) *Date and Place of Birth*: Corroboration of date and place of birth through a check of appropriate documentation; a check of Bureau of Vital Statistics records when any discrepancy is found to exist.

(e) *Citizenship*: For individuals born outside the United States, verification of US citizenship directly from the appropriate registration authority; verification of US citizenship or legal status of foreign-born immediate family members (spouse, cohabitant, father, mother, sons, daughters, brothers, sisters).

(f) *Education*: Corroboration of most recent or most significant claimed attendance, degree, or diploma. Interviews of appropriate educational sources if education is a primary activity of the subject during the most recent three years.

(g) *Employment*: Verification of all employment for the past seven years; personal interviews of sources (supervisors, coworkers, or both) for each employment of six months or more; corroboration through records or sources of all periods of unemployment exceeding sixty days; verification of all prior federal and military service, including discharge type. For military members, all service within one branch of the armed forces will be considered as one employment, regardless of assignments.

(h) *References*: Four references, of whom at least two are developed; to the extent practicable, all should have social knowledge of the subject and collectively span at least the last seven years.

(i) *Former Spouse*: An interview of any former spouse divorced within the last ten years.

(j) *Neighborhoods*: Confirmation of all residences for the last three years through appropriate interviews with neighbors and through record reviews.

(k) *Financial Review*: Verification of the subject's financial status, including credit bureau checks covering all locations where subject has resided, been employed, and/or attended school for six months or more for the last seven years.

(l) *Local Agency Checks*: A check of appropriate criminal history records covering all locations where, for the last ten years, the subject has resided, been employed, and/or attended school for six months or more, including current residence regardless of duration. (**NOTE:** If no residence, employment or education exceeds six months, local agency checks should be performed as deemed appropriate.)

(m) *Public Records*: Verification of divorces, bankruptcies, and other court actions, whether civil or criminal, involving the subject.

(n) *Subject Interview*: A subject interview, conducted by trained security, investigative, or counterintelligence personnel. During the investigation, additional subject interviews may be conducted to collect relevant information, to resolve significant inconsistencies, or both. Sworn statements and unsworn declarations may be taken whenever appropriate.

(0) *Polygraph* (only in agencies with approved personnel security polygraph programs): In departments or agencies with policies sanctioning the use of the polygraph for personnel security purposes, the investigation may include a polygraph examination, conducted by a qualified polygraph examiner.

14. ***Expanding the Investigation***. The investigation may be expanded as necessary. As appropriate, interviews with anyone able to provide information or to resolve issues, including but not limited to cohabitants, relatives, psychiatrists, psychologists, other medical professionals, and law enforcement professionals may be conducted.

STANDARD C

Single-Scope Background Investigation-Periodic Reinvestigation (SSBI-PR)

15. ***Applicability.*** Standard C applies to reinvestigations for:

(a) *Access to TOP SECRET* (including TOP SECRET Special Access Programs) and Sensitive Compartmented Information; and

(b) *"Q" access authorizations*.

16. ***When to Reinvestigate***. The reinvestigation may be initiated at any time following completion of, but not later than five years from the date of, the previous investigation (see Table 2).

17. ***Reinvestigative Requirements.*** Requirements are as follows:

(a) *Completion of Forms*: Completion of Standard Form 86, including applicable releases and supporting documentation.

(b) *National Agency Check*: Completion of a National Agency Check (fingerprint cards are required only if there has not been a previous valid technical check of the FBI).

(c) National Agency Check for the Spouse or Cohabitant (if applicable): Completion of a National Agency Check, without fingerprint cards, for the spouse or cohabitant. The National Agency Check for the spouse or cohabitant is not required if already completed in conjunction with a previous investigation or reinvestigation.

(d) *Employment:* Verification of all employment since the last investigation. Attempts to interview a sufficient number of sources (supervisors, coworkers, or both) at all employments of six months or more. For military members, all service within one branch of the armed forces will be considered as one employment, regardless of assignments.

(e) *References*: Interviews with two character references who are knowledgeable of the subject; at least one will be a developed reference. To the extent practical, both should have social knowledge of the subject and collectively span the entire period of the reinvestigation. As appropriate, additional interviews may be conducted, including with cohabitants and relatives.

(f) *Neighborhoods:* Interviews of two neighbors in the vicinity of the subject's most recent residence of six months or more. Conformation of current residence regardless of length.

(g) *Financial Review*:

(1) *Financial Status*: Verification of the subject's financial status, including credit bureau checks covering all locations where subject has resided, been employed, and/or attended school for six months or more for the period covered by the reinvestigation;

(2) *Check the Treasury's Financial Data Base*: Agencies may request the Department of the Treasury, under terms and conditions prescribed by the Secretary of the Treasury, to search automated data bases consisting of reports of currency transactions by financial institutions, international transportation of currency or monetary instruments, foreign bank and financial accounts, and transactions under $10,000 that are reported as possible money laundering violations.

(h) *Local Agency Checks*: A check of appropriate criminal history records covering all locations where, during the period covered by the reinvestigation, the subject has resided, been employed, and/or attended school for six months or more, including current residence regardless

of duration. (NOTE: If no residence, employment or education exceeds six months, local agency checks should be performed as deemed appropriate.)

(i) *Former Spouse*: An interview with any former spouse unless the divorce took place before the data of the last investigation or reinvestigation.

(j) *Public Records*: Verification of divorces, bankruptcies, and other court actions, whether civil or criminal, involving the subject since the date of the last investigation.

(k) *Subject interview*: A subject interview, conducted by trained security, investigative, or counterintelligence personnel. During the reinvestigation, additional subject interviews may be conducted to collect relevant information, to resolve significant inconsistencies, or both. Sworn statements ands unsworn declarations may be taken whenever appropriate.

18. ***Expanding the Reinvestigation***. The reinvestigation may be expanded as necessary. As appropriate, interviews with anyone able to provide information or to resolve issues, including but not limited to cohabitants, relatives, psychiatrists, psychologists, other medial professionals, and law enforcement professionals may be conducted.

Investigative Standards for Temporary Eligibility for Access

1. ***Introduction***. The following minimum investigative standards, implementing section 3.3 of Executive Order 12968, *Access to Classified Information*, are established for all United States Government and military personnel, consultants, contractors, subcontractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information before the appropriate investigation can be completed and a final determination made.

2. ***Temporary Eligibility for Access***. Based on a justified need meeting the requirements of sect. 3.3 of Executive Order 12968, temporary eligibility for access may be granted before investigations are complete and favorably adjudicated, where official functions must be performed prior to completion of the investigation and adjudication process. The temporary eligibility will be valid until completion of the investigation and adjudication; however, the agency granting it may revoke it at any time based on unfavorable information identified in the course of the investigation.

3. ***Temporary Eligibility for Access at the CONFIDENTIAL and SECRET levels and Temporary Eligibility for "L" Access Authorization***. As a minimum, such temporary eligibility requires completion of the Standard Form 86, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, and submission of a request for an expedited National Agency Check with Local Agency Checks and Credit (NACLC).

4. ***Temporary Eligibility for Access at the TOP SECRET and SCI Levels and Temporary Eligibility for "Q" Access Authorization:*** *For Someone Who Is the Subject of a Favorable Investigation Not Meeting the Investigative Standards for Access at Those Levels*. As a minimum, such temporary eligibility requires completion of the Standard Form 86, including any applicable supporting documentation, favorable review of the form by the appropriate

adjudicating authority, and expedited submission of a request for a Single Scope Background Investigation (SSBI).

5. ***Temporary Eligibility for Access at the TOP SECRET and SCI Levels and Temporary Eligibility for "Q" Access Authorization***: *For Someone Who Is Not the Subject of a Current, Favorable Personnel or Personnel-Security Investigation of Any Kind*. As a minimum, such temporary eligibility requires completion of the Standard Form 86, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, immediate submission of a request for an expedited Single Scope Background Investigation (SSBI), and completion and favorable review by the appropriate adjudicating authority of relevant criminal history and investigative records of the Federal Bureau of Investigation and of information in the Security/Suitability Investigations Index (SII) and the Defense Clearance and Investigations Index (DCII).

6. ***Additional Requirements by Agencies*.** Temporary eligibility for access must satisfy these minimum investigative standards, but agency heads may establish additional requirements based on the sensitivity of the particular, identified categories of classified information necessary to perform the lawful and authorized functions that are the basis for granting temporary eligibility for access. However, **no** additional requirements shall exceed the common standards for background investigations developed under section 3.2(b) of Executive Order 12968, Temporary eligibility for access is valid only at the agency granting it and at other agencies who expressly agree to accept it and acknowledge understanding of its investigative basis. It is further subject to limitations specified in sections 2.4(d) and 3.3 of Executive Order 12968 *Access to Classified Information.*

MILITARY PERSONNEL SECURITY PROGRAM EVALUATION CHECK SHEET

A COMMENT IS REQUIRED IN THE COMMENTS SECTION FOR ALL ITEMS DEEMED "NOT APPLICABLE".

UNIT_____ DATE CONDUCTED:_____
COMMAND SECURITY OFFICER:_____
EVALUATOR:_____

	PAGE REF	YES	NO
Does command ensure a members need for security clearance/access is reviewed upon arrival?		____	____
Are personnel assigned to duties requiring access to classified information properly indoctrinated?		____	____
Are all personnel assigned to sensitive duties or access to classified information U.S. citizens?		____	____
Is U.S. citizenship verified prior to granting a final security clearance?		____	____
Are personnel selected to head delegations from the U.S. the subject of an SSBI?		____	____
Are Coast Guard representatives at international conferences the subject of an NAC?		____	____
Do commands conduct a self evaluation annually and submit copies to the cognizant security manager?		____	____
Are investigation requirements met for personnel requiring clearance?		____	____
Does the CSO review the CGHRMS control report?		____	____
Does the CSO maintain a command roster of all personnel granted access to classified material?		____	____
Does the roster contain all of the required information?		____	____
When an individual requires clearance/access, does the command ensure that all conditions are met prior to utilizing a previous central adjudication facility (CAF) determination?		____	____

Is the appropriate entry made on a properly completed CG-5588 for security clearance re-approval?	____ ____
Does the commanding officer sign the CG-5588 re-approving clearances for new personnel?	____ ____
Is the CG-5588 and other appropriate documents filed in the members PDR?	____ ____
Is the number of personnel granted access to classified information kept to an absolute minimum?	____ ____
If significant derogatory information is discovered on a cleared individual, is access suspended pending resolution?	____ ____
Does the command ensure that access is not granted solely to permit entry to or ease of movement within controlled areas?	____ ____
Does the command ensure that access is not granted merely as a result of any particular title, rank, position, or affiliation?	____ ____
Is access to classified information granted only to personnel for whom an appropriate investigation has been completed?	____ ____
Are proper procedures followed when granting an interim secret/confidential clearance?	____ ____
Are proper procedures followed when granting an interim top secret clearance?	_____ ____
Are interim clearances extended as necessary?	____ ____
Is the standard clearance notification letter sent when visiting other commands?	____ ____
Are NACLC requests reviewed by the CSO and submitted properly?	____ ____
Are SSBI requests justified, reviewed by the CSO for correctness and completeness and submitted to the cognizant security manager?	____ ____
When completing the SF-86 for an SSBI are the appropriate questions answered with a 10-year scope?	____ ____
Is a certificate of clearance and copy of an SF-312 filed in the PDR of members with a security clearance?	____ ____
Were all CG-5274's sent to CGPC for filing in the individuals permanent record?	____ ____

Does the command security officer notify the SSO if a letter of intent to deny or revoke clearance is received on an individual with SCI access?	____	____
Does the command ensure that individuals sign and forward acknowledgement portion of letters of intent when received?	____	____
Are individuals briefed on the effect of failure to appeal a security clearance determination?	____	____
Are the appropriate procedures followed when temporary access is granted?	____	____
Is derogatory information reported as part of the continuous evaluation program?	____	____
When a Coast Guard member marries or cohabits with a foreign born non-U.S. citizen is an SF-86 completed on the cohabitant as required?	____	____
Are all members of the command briefed from time to time on their responsibility in regards to classified and sensitive information?	____	____
Are all personnel reporting aboard the unit given an arrival briefing?	____	____
Are personnel who have access to classified information given an initial access briefing?	____	____
Have all personnel who have been granted access executed an SF-312 non-disclosure agreement?	____	____
Is the SF-312 properly accepted?	____	____
Are original SF-312's sent to Commandant (CGPC-ADM3) with a copy filed in the members PDR?	____	____
Are all personnel traveling to a foreign country given a foreign travel briefing?	____	____
Are all personnel who have access given an annual refresher brief?	____	____
Are personnel terminating government service given a final termination briefing?	____	____
Are briefings developed and documented correctly?	____	____
Are suicides and attempted suicides reported as required?	____	____
Are unauthorized absences reported as required?	____	____
Are Coast Guard personnel aware of techniques employed by foreign intelligence activities in attempting to obtain classified information?	____	____

Are individuals aware of their responsibilities when becoming aware of possible acts of sabotage, espionage or deliberate compromise of classified information? ____ ____

COMMENTS:_____
_____
_____
_____
_____

EVALUATOR
COMMENTS:_____
_____
_____
_____
_____

THIS EVALUATION CHECKLIST IS IN NO WAY INCLUSIVE OF ALL REQUIREMENTS CONTAINED WITHIN THE MANUAL..

CGHRMS DATA BASE SECURITY FIELD CODE DEFINITIONS

CLEARANCE/SECURITY DETERMINATION ELIGIBILITY

A one-character alpha/numeric code to indicate the level of security clearance adjudicated by the central adjudication facility (CAF).

CODE	MEANING
A	No clearance - investigation reopened
B	SCI denied - ineligible for clearance
C	Confidential
D	Clearance denied
E	Interim Confidential
F	SCI revoked - ineligible for clearance
G	Secret - SCI denied
H	Secret - SCI revoked
I	Clearance Pending - investigation reopened
J	No clearance required - file created
K	Eligible for SCI with waiver
L	Restricted to non-sensitive duties-not eligible for sensitive duties
M	Top Secret only - SCI revoked
N	Top Secret only - SCI denied
O	Interim Secret
P	Interim Top Secret
Q	No clearance/access required - favorable investigation
R	Clearance revoked
S	Secret
T	Top Secret
U	Interim SCI
V	DCID 1/14 eligible
W	Top Secret - SCI requires adjudication
X	Action pending
Y	Pending final adjudication/access suspended
Z	Adjudicative action incomplete due to loss of jurisdiction
1	LAA Confidential
2	LAA Secret
3	Pending reply to LOI/Statement of Reasons (SOR)
4	Clearance administratively withdrawn
5	Position of trust (no clearance determination)
6	SCI denied (no clearance determination)
7	SCI revoked (no clearance determination)

SECURITY BRIEFINGS

A. Purpose. The security briefing is a presentation designed to persuade others and ensure all personnel understand their responsibilities for protecting government assets. Briefings should be tailored to meet the specific needs of the unit, as well as those of different groups within the unit.

B. Responsibility. The Command Security Officer (CSO) is responsible for ensuring security briefings are properly conducted and appropriately documented. The CSO may or may not be the individual actually presenting the briefings, but his or her advice and assistance will probably be needed.

C. Types. Listed below are the types of briefings required in the security program. Exhibit 3-1 outlines a summary and schedule of the required briefings.

1. Arrival Briefing. All personnel reporting aboard the unit shall be given an arrival briefing. The briefing shall (at a minimum) inform personnel of security points of contact, internal security procedures, Operations Security (OPSEC), loss/crime prevention responsibilities, what classified information is, how to identify it, how and why it is protected, and actions to take if an individual discovers it unattended. Exhibit 3-2 provides a sample briefing.

2. Access Briefing. Personnel who will have access to classified information shall be given an access briefing after receiving an interim or final clearance, but prior to being assigned duties that require access to classified information. The briefing shall inform personnel of their security responsibilities in protecting the information, including the laws applicable to the unauthorized disclosure of classified information. Exhibit 3-3 provides a sample briefing. The access briefing may be combined with the arrival briefing.

3. Coast Guard Level I AT/FP Briefing. Personnel (with or without access to classified information) traveling to a foreign country while on leave, authorized absence or official orders shall be given a Level I AT/FP briefing. At a minimum, those who travel shall be briefed at least annually. This briefing consists of two parts the formal briefing (good for 12 months) and the current Intelligence on the destination (this is required before every trip prior to departure). The briefing shall inform personnel of general precautions for personal safety. An official debrief is not required. However, suspicious incidents shall be reported to G-CFI via the cognizant security manager (SECMGR). Exhibit 3-4 provides a sample briefing.

4. Counter Espionage (CE) Awareness Briefing. Any individual who has access to classified information, and plans to travel to or through a criteria country or to attend a meeting in the United States or elsewhere, in which representatives of criteria countries are expected to participate, shall report these plans to the unit, and shall be given a CE awareness briefing. At a minimum, those who travel or attend such meetings shall be briefed at least annually. The briefing shall inform personnel of possible exploitation attempts by foreign intelligence services and general precautions for personal safety. Exhibit 3-5 provides a sample briefing.

5. Counter Espionage (CE) Awareness Debriefing. When the individual returns, he or she shall be debriefed to provide the opportunity to report any incident - no matter how insignificant it may have seemed. Information that may have security implications shall be reported to G-CFI via the cognizant SECMGR. Exhibit 3-6 provides a sample briefing.

6. Annual Refresher Briefing. Once a year, all personnel shall be given a refresher briefing. The briefing may address general security matters, changes in policies or procedures, specific problem areas, etc., but shall be tailored to the specific needs of the target audience. Therefore, it is not possible to provide a sample refresher briefing. Some suggested topics to cover may be OPSEC, counter espionage reminders, AT/FP Level I, reporting of possible compromises and missing, lost or stolen government property, hand-carrying of classified material, crime prevention, factors affecting personnel security clearance adjudication, past year statistical data, etc. The list is endless; the intent is to tailor the briefing based on specific needs, problem areas, etc., and stimulate security consciousness by periodic re-emphasis of the basic security principals.

7. Transfer Briefing. At the time of transfer from a particular unit, all personnel who have access to classified information at their present unit shall be given a transfer briefing. The briefing shall inform personnel that their present clearance is administratively withdrawn without prejudice; all classified material must be returned; and the individual is no longer authorized access. Exhibit 3-7 provides a sample briefing.

8. Final Termination Briefing. Personnel shall be given a termination briefing upon termination of government service, or when a clearance is revoked for cause. The briefing shall remind personnel to return all classified material in his or her possession, and that they remain subject to the provisions of the criminal code and other applicable laws relating to the unauthorized disclosure of classified information. Exhibit 3-8 provides a sample briefing.

D. Record of Briefings. Briefings shall be recorded on the Personnel Security Record (CG-5274) for both military and civilian personnel. However, when large numbers of personnel are briefed at one time, such as for a refresher briefing or counterintelligence awareness briefing, a letter or memorandum signed by the commanding officer, with a list of personnel in attendance (such as a sailing list), may be attached to the CG-5274. The final termination briefing for civilians shall be recorded on the Security Termination Statement (DOT 1600.10).

EXHIBIT 3-2

ARRIVAL BRIEFING

INTRODUCTION

Welcome! A special congratulation on your new assignment. Your job makes you a member of a very special team comprised of military and civilian personnel who are engaged in work, which impacts the defense of our great country.

In performing your job, you will be dealing (at a minimum) with unclassified, sensitive and Unclassified and For Official Use Only (FOUO) information. You may also be working with information which has been classified in the interest of our national security - that is, information which is CONFIDENTIAL, SECRET, OR TOP SECRET. Security shall become a vital part of your daily routine and it is essential you know and understand the requirements for protecting government assets (unclassified information, FOUO information, classified information, property and personnel).

I mentioned you are part of a team. I know in some area of your life you have learned how important teamwork is to the final outcome of any event. Every individual must do his or her part if the team is to win. And this team must win. We have established a security program to protect government assets (both personnel and property) and to prevent our adversaries from gaining access to Coast Guard information. However, no matter how comprehensive the program may be, the key ingredient is **people**. You and your coworkers will ultimately determine the success of our established procedures. Your daily security vigilance helps us keep our national security advantage and protects the freedoms we all enjoy so much.

NOTE: At this time, inform the individual of security points of contact at the unit; e.g., Command Security Officer (CSO), Classified Material Control Officer (CMCO), Area and District Security Manager (SECMGR), Unit Automated Data Processing Systems Security Officer (ADPSSO), etc. Advise them of other information specific to the unit, e.g., where security regulations can be located, where to report security incidents, etc.

PERSONNEL SECURITY

Personnel Security is the system by which we assure that everyone employed by the Coast Guard meets certain standards. Prior to reporting to work, unless you transferred from a Coast Guard unit or other government agency, you were asked to fill out certain forms concerning your background. An appropriate investigation was conducted to determine your suitability for employment with the Coast Guard, and to determine your eligibility for a security clearance (if required). Not every employee will require a security clearance. A person with a security clearance at one unit may transfer to another unit and not be issued a clearance, or may be granted a clearance at a level lower than the one previously held. It all depends on the needs in your current position. Questionable information collected during the investigation must be clarified and may require further investigation. The information obtained must be evaluated and a common sense determination made taking into consideration all available information. Questionable factors include criminal conduct,

alcohol abuse, drug abuse, financial irresponsibility, and falsification of information provided in interviews or on employment forms, or any other factor that would cast in doubt an individual's responsibility, loyalty, reliability or trustworthiness.

Evaluation of your character and activities doesn't end after the initial investigation. We have a program that requires a continuing evaluation of your eligibility to hold a security clearance. Your actions can affect your ability to retain a security clearance, and possibly your position. We've learned that one of the greatest threats to our security comes from our own carelessness and complacency.

It takes your cooperation to make this continuous evaluation program work. You have a responsibility to report to your CSO any questionable information that indicates an individual no longer meets the security standards for eligibility to hold a security clearance. You may feel a little uncomfortable about reporting a coworker, but keep in mind the importance of security interests, as well as national security interests, and the good of the entire country. If that person is compromising Coast Guard security, it affects not only the whole U.S. security program, but you and your family as well.

INFORMATION SECURITY

Executive Order 12958 prescribes a uniform system for safeguarding national security information. Classified information is official information that requires protection against unauthorized disclosure in the interest of national security. Unauthorized disclosure occurs when someone who is not authorized by the government to have access to classified information does get access, either accidentally or intentionally.

Access to classified information is permitted only to persons who possess an appropriate security clearance and an official need-to-know. Your position may or may not require access to classified information. If it does, further information will be provided to you during an "access briefing". If not, this section is provided in case you inadvertently discover unprotected classified material, you will be able to identify it and properly protect it.

There are three categories of classified information that require specified protective measures; the unauthorized disclosure of this information will result in a degree of damage to the national security:

- TOP SECRET - The unauthorized disclosure of this information could reasonably be expected to cause "exceptionally grave damage" to our national security.

- SECRET - The unauthorized disclosure of this information could reasonably be expected to cause "serious damage" to our national security.

- CONFIDENTIAL - The unauthorized disclosure of this information could reasonably be expected to cause "damage" to our national security.

All documents containing classified information will be marked in a prescribed manner to indicate the classification assigned and the degree and duration of protection required. Classification levels will be conspicuously marked or stamped at the top and bottom of all

pages. Paragraphs, subjects and titles will be individually marked with parenthetical symbols (TS), (S), or (C). The face of the document will also include "Classified by" and "Declassify on" lines to identify classification sources and declassification and downgrading instructions.

Classified material will be stored in approved secure areas, in GSA approved security containers or under the direct observation of authorized personnel. If by chance, you discover classified material unprotected, i.e., in an incoming mail box, in a copier machine, on top of a file cabinet, on a desk, etc., you have an immediate responsibility to protect the material from further risk and report the incident to your CSO. If you cannot both protect the information and report the incident, have someone else make the report while you continue to protect the information.

If you are approached by anyone seeking unauthorized access to classified or sensitive information, immediately report it to your CSO. It is no secret that dedicated foreign intelligence services are working in this country to gain valuable information. Compromised classified information could severely damage America's national security; we must all work together to prevent this from happening.

LOSS/CRIME PREVENTION

Care must be taken to ensure that adequate safeguards are established to protect government property from loss or theft. Items considered being highly susceptible to loss or theft includes calculators, small office machines, transistor radios, desk clocks, postage stamps, etc. Government funds, controlled medical substances, arms, ammunition and explosives, sensitive forms such as un-issued identification cards, purchase orders, and credit cards are also highly susceptible to loss or theft. Careless handling of these items encourage thievery or contributes to their inadvertent loss.

Concern is not only focused on the external threat of criminal activity; it is specifically directed toward the internal threat: theft and pilferage by those who have authorized access, inattention to physical security practices and disregard for property control and accountability.

You have a responsibility to immediately report to your CSO any missing, lost or stolen government property. Timely reporting increases the possibility that property will be recovered. Reporting losses provides a measure of effectiveness for internal controls, stimulates reviews of inventory and accountability procedures, and reflects both strengths and weaknesses in the security program.

You can support the loss prevention effort by observing the following precautions:

- Lock up all small items at the close of business.
- Do not leave money or other valuables in desk drawers.
- Keep your purse or wallet with you at all times.
- Make sure coat/clothing racks are well within controlled spaces, not close to exterior doors or open hallways.

- Require all unknown persons who enter your space to identify themselves. Verify their reason for being there if you are not sure.

- Report missing, lost or stolen government property, including identification badges and keys.

- If you observe any suspicious persons or activities in buildings, parking areas, etc., immediately report it to your CSO

OPERATIONS SECURITY

Operations Security (OPSEC) is a process which identifies what unclassified and sensitive information needs protecting, where the information can be vulnerable to collection by an adversary, and what actions we can take to protect information related to our projects, plans and operations. OPSEC is concerned with the protection of all information which could be useful to a known adversary. We must recognize that information can be gathered through written and verbal communication, visual observations, and technical surveillance gathering methods.

The OPSEC process looks at the entire operation and the threats, vulnerabilities and the countermeasures associated with a project, program, exercise or operation. The process pays particular attention to how we do things. It considers all the traditional programs and defines weaknesses not collectively addressed by those programs.

OPSEC planning efforts are coordinated with OPSEC representatives, technical employees, and security specialists. During planning, the OPSEC process identifies information requiring protection and the detectable activities that may reveal the information we want to protect. Detectable activities are considered vulnerabilities that require countermeasures.

You can support the OPSEC effort by being aware of what information you need to protect, complying with OPSEC instructions and plans, and coordinating OPSEC issues with your OPSEC representatives.

CONCLUSION

Security's mission is to establish an awareness of good security practices on the part of all employees and to ensure compliance with government policies and procedures designed to protect unclassified, sensitive and classified information, property and personnel. Security is here to help you. Here's how you can help us:

- Understand your individual security responsibilities.

- Make security a daily habit.

- Ask if you have any questions, or need help.

Security depends on your cooperation and personal awareness. You are asked to take an active part in protecting your country's vital secrets, property and personnel. You are asked to keep your sense of security awareness strong. You must choose to do what you know is right, now and for the future.

EXHIBIT 3-3

ACCESS BRIEFING

INTRODUCTION

Competent authority has determined that you require access to classified information in the performance of your official duties. You are now in a position of high public trust. As a government employee, the standards of conduct required of you are higher than for other U.S. citizens. Your conduct reflects not only on you personally, it also reflects on your unit and the Coast Guard. The trust placed in you should be exemplified by your daily efforts as a member of our security team.

Access to classified information is permitted only to persons who possess an appropriate security clearance and who have an **official need-to-know**. Access means the ability and opportunity to obtain knowledge or possession of classified information.

A security clearance is an administrative determination, based on an appropriate investigation, that you are trustworthy and eligible for access to classified information. If you have been granted a TOP SECRET clearance, you are eligible for access to Top Secret, Secret and Confidential information. If you have been granted a SECRET clearance, you are eligible for access to Secret and Confidential information. If you have been granted a CONFIDENTIAL clearance, you are eligible for access to Confidential information only.

Whether you are given access depends on the information you need-to-know to do your job. **Need-to-know** is a determination that you have a requirement for access to classified information to accomplish your official duties. You are not only responsible for restricting your own access to that which you need-to-know, but also for making sure that others are properly cleared and have a **need-to-know** before you release the information to them.

ORIGINAL AND DERIVATIVE CLASSIFICATION

There are two types of classification, Original and Derivative. Original classification is the initial determination that information requires protection in the interest of national security. Original classification is only required when new information is developed which cannot reasonably derive its classification from other classified or related information. Only those officials who have been specifically delegated original classification authority (in writing) may make original classification decisions. Remember, in peacetime, only Commandant (G-C) and (G-O) have original classification authority.

Derivative classification is simply classifying information based on a previous original classification decision. Your information may be derived from an original classification action, from a classified source document or classification guide. You may be incorporating, paraphrasing, summarizing, or restating that information, but your classification is a result of that previous original classification decision, and is therefore, a derivative classification.

Remember that information should be classified at the lowest appropriate classification level and should be downgraded (classification lowered) or declassified (classification removed) at the earliest possible date.

MARKING

All documents containing classified information shall be marked in a prescribed manner to indicate the classification level assigned and the degree and duration of protection required. The main purpose of marking is to ensure that there is no doubt in the user's mind as to the classification of the specified material. These markings are the very minimum required for classified documents. COMDTINST M5510.23, Classified Information Management Program, contains more detailed marking instructions and notices.

The overall classification shall be conspicuously marked or stamped on the face and back cover of the document. Each interior page shall be marked at the top and bottom with the highest classification of information on that page, or with the overall classification of the entire document.

Each paragraph shall be marked to show the level of classification or that it is unclassified. The parenthetical symbols (TS) for Top Secret, (S) for Secret, (C) for Confidential, and (U) for Unclassified shall be placed immediately preceding the text it governs. Subjects or titles shall also be marked immediately following and to the right of the subject or title with these parenthetical symbols.

Each face of a classified document shall be marked to show the name and title of the classifier, the source of classification, and the date for any downgrading or declassification action.

SAFEGUARDING

All classified material received or transmitted by the unit shall be processed through a designated Security Control Point (SCP) for accountability purposes. The SCP prepares receipts and accountability records and forwards the classified material to the proper office for the necessary action. However, YOU are the key player in this system. All the records and receipts are meaningless unless YOU know how to safeguard the information. Some important points to remember:

- Only persons with an appropriate security clearance and need-to-know are authorized access to classified information.
-

- Classified material shall be stored in approved secure areas, in GSA approved security containers or under the direct observation of authorized personnel.

- Security container combinations shall be protected the same as classified material and stored appropriately (never in wallets, desks, calendars, etc.) Combinations shall be changed as often as necessary, but at least annually. Only a minimum number of people shall have access to the combination.

- When removed from storage, classified documents shall have a standard form cover sheet (SF 703, 704, 705) attached.

- Classified information shall not be read or discussed in public places or in the presence of unauthorized personnel.

- Contrary to popular belief, there is no requirement to only discuss classified information in a designated classified space.

- It would be unreasonable to expect two employees sharing an office and working on the same project not to talk about what they are doing and go to a classified space. What is required is that employees take reasonable precautions to ensure that only authorized ears hear what is discussed. Look around to see who is within hearing range. Never have discussions near open doors or windows, or when someone is using the telephone.

- Non-secure telephones continue to be the most widely exploited communications instrument; continuous caution and awareness of their vulnerabilities is a must. Classified discussions over non-secure telephones are prohibited. Telephones and telephone systems are subject to communications security monitoring. Classified discussions shall only be over approved telephone systems, e.g., the STU III. Use of the STU III is also encouraged when discussing sensitive information and operational matters.

- Reproduction shall be held to an absolute minimum and only on authorized machines. Reproduced copies shall be controlled and accounted for the same as original documents.

- Classified material shall be destroyed when there is no longer an operational need for it. Directives, Publications and Reports Index, COMDTINST M5600, will aid in determining holding requirements. Security containers are expensive and accountability procedures are time consuming; the less classified material you have the better.

- A system of double security checks (utilizing SF 701) shall be employed at the close of business to ensure all classified information is properly secured.

- Classified material shall not be removed from the unit unless specifically authorized by the commanding officer. It shall never be taken home.

- Transmit classified material only by approved methods. Only hand-carry it when it is not available at your destination or when time or other constraints dictate. This practice is generally discouraged due to concerns of hijacking, accidents and human error (e.g., forgetting briefcases). Rather than hand-carry the material on your return trip, mail it back to your unit.

ADMINISTRATIVE SECURITY DISCREPANCIES AND COMPROMISES

Administrative security discrepancies are, in simple terms, not following security regulations/procedures. They fall under two categories: Those that result in a compromise or possible compromise of classified information, and those in which security regulations/procedures have been violated but do not result in a compromise or possible compromise.

A compromise is simply disclosing classified information to anyone who does not have the appropriate security clearance or need-to-know. Another term for compromise is unauthorized disclosure.
Everyone would prefer to avoid these infractions, but they happen in the best of places. And when they happen, you have the responsibility to immediately report the incident to your Command Security Officer (CSO).

These infractions must be vigorously investigated so that the cause can be identified and corrected; and we can determine what damage may have been done and take appropriate actions to minimize the damage. Timely reports, reflected through inquiry and conscientious corrective action, will be recognized as one of the best indicators of a security-conscious work force and a well-managed security program.

TRAVEL TO FOREIGN COUNTRIES

You have the responsibility to notify your CSO prior to any travel outside the U.S. so that you may be given the proper security briefings. These briefings will inform you of general security precautions, safety tips, and possible intelligence-gathering methods and potential hazards you may be exposed to.

THE FOREIGN INTELLIGENCE THREAT

The foreign intelligence threat arrayed against the U.S. is pervasive and confronts the government and our nation's industry with increasingly serious challenges. This threat continues despite the end of the Cold War. Foreign intelligence services depend to a large degree on their human collection networks throughout the world to satisfy their requirements for U.S. advanced technology. Persons are recruited, or volunteer, to provide information to foreign intelligence services.

You have the responsibility to report to your CSO any attempts by any unauthorized individual to solicit classified or sensitive information. Additionally, you must report to your CSO any attempts by representatives of foreign country to:

- Establish a personal or professional relationship.

- Obtain information through monetary payments, bribery, observation, collection of documents, or by personal contact.

- Coerce personnel by blackmail, threats against or promises of assistance to relatives living under their control.

- Exploit discontented personnel or those with personal difficulties.

- Intimidate, harass, entrap, discredit, search, spy on, or recruit personnel.

- Induce personnel to defect or induce those who have fled from another country to re-defect.

NONDISCLOSURE AGREEMENT SF 312

You will now be asked to sign the SF 312 as a condition of access to classified information. The SF 312 is a contractual agreement between the U.S. Government and you, in which you agree to never disclose classified information to an unauthorized person (now or beyond your employment with the Coast Guard). Its primary purpose is to inform you of the trust that is placed in you by providing you access to classified information; your responsibilities to protect that information from unauthorized disclosure; and the consequences that may result from your failure to meet those responsibilities. If you knowingly, willfully, or negligently disclose classified information to unauthorized persons, you are subject to a wide range of administrative sanctions, civil remedies, and criminal prosecutions.

NOTE: The SF 312 is to be signed only upon first time access to classified information, or if previously unexecuted.

EXHIBIT 3-4

COAST GUARD LEVEL I AT/FP BRIEFING

Planning a trip overseas is always worrisome. Whether for official travel or pleasure, we worry about what to take and what not to take; tickets, passports, money, etc. Recently, we've had another worry - terrorism. Throughout the world, terrorism has become a means whereby weaker governments or political groups try to force their beliefs and goals upon others. International terrorism is REAL and has touched the lives of many Americans when least expected. However, terrorism is not the only problem overseas travelers face today. Death and injury also occur during acts of random violence spawned by ethnic differences, extremism, fundamentalism, political violence, poverty and tribalism. We cannot make ourselves immune from terrorism anymore than we can from ordinary criminal violence. But the same precautions taken in a personal crime prevention program will serve to deter terrorist as well.

The information presented in this briefing is for your personal safety. Security must be implemented to ensure continued safety in foreign environments. Each country and each circumstance will present you with a unique situation. Individual precautions can substantially reduce the possibility of a successful criminal or terrorist attack and could make a difference in your survival.

BEFORE YOU GO

- Being self-informed is important. Learn about your destination, its history, culture, local customs and laws. This can be done by consulting your local travel agent, library, or talking to people who have been there.

- Call the Bureau of Consular Affairs Office of Public Affairs 202-647-5225 or the Web Site http://travel.state.gov/travel_warnings.html. The hot-line provides up-to-date information concerning potential threats to Americans generated by political disorder, crime, health risks, and other possible problems that travelers may face. Another good source is the Center for Disease Control Travelers Warning at the new toll-free number is 877-FYI-TRIP. The toll-free fax number for requesting information is 888-232-3299 or www.cdc.gov/travel.

- Check the calendar. Terrorists often carry out attacks on days commemorating significant events in their regions, religious holidays or on anniversaries of previous attacks.

- Choose your airline carefully. Some are more likely to be targeted than others. The safest airlines tend to be those from such countries as Sweden, Switzerland, Singapore and Hong Kong, (which are not members of political blocs or embroiled in localized conflicts).

- All references during travel arrangements should be made without military rank.

- Try to fly on a larger plane if possible. Skyjacking a larger plane requires more planning, manpower and effort.

- **Coach is safer than first class**. Terrorists tend to use first class as their command post. You would be closer to them if they decided to open fire. Should there be a rescue attempt, you run a greater risk of being caught in a crossfire. It's easier to blend into the crowd in coach.

- Avoid aisle seats. Passengers on the aisle are generally subjected to the most abuse. If a rescue operation takes place, most of the shooting would be directed down the aisles.

- In the event your return is delayed, make sure your personal matters are in good order and accessible to your spouse (or designee) prior to your departure, e.g., power of attorney, insurance policies, important papers, safe deposit box, joint bank accounts, updated will, etc.

- Before leaving, you may want to have a frank discussion with your family concerning appropriate actions in the event your return is delayed.

LUGGAGE AND PACKING

- Travel light. Take what you'll need, but nothing more.
- Don't take flashy clothes or jewelry that will draw unnecessary attention to yourself.
- Avoid packing anything that is breakable, high value, indispensable or of sentimental value. Don't take anything you can't afford to lose.
- Have your name and address (never with your military affiliation) on the inside and outside of each piece of luggage.
- Pack eyeglasses and important documents in a small carry-on piece of luggage and keep it with you.
- Leave official orders or papers in your checked in luggage and not on your person.
- Only take essential identification with you (passport, shot records, drivers license, military ID, etc.). Leave building passes, security badges, military club cards, etc. at home.
- Don't advertise your religious, ethnic or military affiliation. Don't wear or take distinctively American apparel or clothing with military patches or insignia. Keep tattoos covered.
- Have an ample supply of all necessary prescription medications in your carry-on luggage. In addition to the normal risk of separation from your checked luggage, this precaution could be a lifesaver if you have to endure a long hijacking. Keep medicines in their original labeled container to make customs processing easier. Also carry a card specifying your blood type and necessary medical information.

AT THE AIRPORT

- Don't linger in the main terminal area. Airport crowds repeatedly have been targeted by terrorists who simply open up with automatic weapons and grenades. Check in quickly, go through immigration and security checks, and wait in a secured passenger area for your flight.
- Check your bags at the counter, not at the curbside. Lock them to prevent someone from slipping drugs or a bomb inside. If a stranger asks you to carry something aboard the plane, refuse and notify appropriate security officials.
- Avoid discussing official business within hearing of other passengers. Do not address each other by rank.

- Sit with your back to a wall. This way you can see everything that's going on.

- Avoid sitting near windows. Try to stand or sit near pillars that provide cover. Be aware of your surroundings. Notice vending machines, sofas and other objects that you could duck behind.

- Stay away from unattended bags. Also avoid trash bins, telephone booths and other enclosures that could contain an explosive device.

- If caught in an open area during a terrorist attack, the best action to take is to immediately drop to the ground and pull your arms over your head the instant you hear shooting or explosions.

- If anything looks suspicious, notify authorities. It is amazing how often passengers have picked out terrorists and hijackers in their midst before an attack occurs but didn't say anything for fear of offending the person. Most Americans are too polite. Don't be bashful about any passenger who behaves peculiarly or looks out of place.

IN THE AIR

- Once seated, be sure to identify the location of the emergency exits.

- On a foreign carrier, avoid speaking English as much as possible. Sit quietly and don't draw attention to yourself.

- Memorize your passport number and other essential information in order to avoid flashing your passport around when filling out landing cards.

- Keep your seat belt on. If a bomb goes off in the plane there will probably be sudden decompression in the cabin, with people and objects being drawn toward the hole.

- Some airlines carry sky marshals. They may attempt to prevent a hijacking. Be prepared to drop to the floor or to scrunch down and cover up if gunfire starts. Whatever you do, don't stand up and look around. - Don't give hijackers any reason to mistake you for a sky marshal. Not all of them may reveal themselves at first. They may remain seated among the passengers, ready to "neutralize" anyone who makes a sudden movement.

- Don't do anything to call attention to yourself. This is the most important rule for surviving a hijacking. Try not to make eye contact with any of the terrorists. Don't complain, protest your detention or destination and don't ask questions. Make yourself inconspicuous. Maintain a neutral composure; give passive cooperation, don't show fear or anger. Only if you require medication or have some other severe medical problem should you let your captors know about you.

- Don't try to reason with your captors. If they are desperate enough to hijack an aircraft, they are capable of reacting unpredictably to the slightest provocation. Take their abuse without complaint. Don't do anything that will force them to react

thoughtlessly, out of their own anger or fear. Should you antagonize them, they may single you out for retribution.

- Don't attempt to gain favor with the terrorists. They generally have little respect for those who grovel. Recognize your responsibility to the other passengers.

- Expect to be uncomfortable; an aluminum cylinder parked on an airport runway can get very hot in the summer and very cold in the winter. You will likely be cramped and stiff. The stench will probably become unbearable. The passengers may not be permitted to use the restrooms and may have to relieve themselves in their seats.

- Take a mental picture of the situation inside the plane. If you are released or escape, authorities will want to know the number of hijackers; their descriptions (gender, nationality, clothing, language); any routines they have established; and the location of hijackers, hostages and weapons or explosives.

- Be alert for possible rescue attempts. Should you hear noises outside the aircraft, don't stare out the window. Get down in your seat and be ready to cover your head or shield your children.

- Don't get involved in a rescue operation; just follow orders. Whatever you do, don't pick up a stray weapon. The assault team may mistake you for one of the hijackers; they will shoot first and ask questions later.

- Watch for terrorists trying to blend in with the passengers if shooting starts. One of the hijackers of an Egypt Air flight to Malta tried to escape by posing as a passenger. Until the situation is under control, the rescuers are likely to treat you roughly. You may be searched. Don't be offended. Comply.

MONEY

- Before you leave, exchange some money for use immediately after you arrive.

- Never exchange money with strangers on the street. It is probably illegal and you could end up in jail.

- Never countersign a travelers check until the moment you're ready to cash it. Each time you cash one, record the number, date and where you cashed it. This is important for a quick refund if lost.

- Carry cash, checks, credit cards and identification on different parts of your person. Money belts are recommended.

- If you are traveling with someone, divide the wealth; each person should carry a portion of the money, travelers checks, credit cards, etc.

HOTELS

- If possible, select a room between the second and eighth floors (too high for easy outside entry and low enough for fire/rescue equipment).

- Better hotels usually have good security and their own security staffs.

- Always keep your windows and doors locked; make a safety check before retiring to ensure they are properly locked.

- Identify emergency exits and stairwells. Know where to locate and how to use the fire extinguisher.

- Make good use of the hotel safe. Put your valuables in the safe and get a receipt for them.

- Don't leave anything of value in your room when you go out, even if it is locked in your suitcase. Don't use a travel lock to secure a drawer containing valuables. It will tell a thief where to look.

- Keep your room in a neat and orderly fashion so you can detect tampering or out of place objects.

- When you leave your room, don't leave indicators showing you are out. Don't tape notes on your door, and don't put a "please make up room" type of sign on the door.

- When out, leave a light on or a radio/TV playing low, in order to deter burglars.

- After dark, keep your curtains and blinds closed. Avoid frequent exposure on balconies.

- Do not answer the phone with your name. Avoid hotel paging.

- Be careful when answering the door; do not answer it automatically. Check by observing through the "peep hole" or an adjacent window.

WALKING

- Avoid walking or jogging alone. Use the "Buddy System". Vary your route.

- Avoid sitting at a sidewalk cafe table or by a window. Know where the emergency exits are.

- Avoid public demonstrations, accidents and other civil disturbances. Ignore taunts and obscene gestures.

- Shun publicity, especially the local news media.

- Do not discuss personal matters such as your travel plans or business dealings with people you don't know.

- Learn useful foreign phrases to request assistance (police, medical, U.S. Embassy, etc.). Keep a phrase book handy.

- Know how to use the local telephones and keep the required coins with you for a pay phone.

- Keep a list of important local phone numbers with you such as police, hotel and U.S. Embassy.

VEHICLE SECURITY

- Vary modes of public transportation whenever possible.

- If possible, choose your own taxi. Use various taxi companies on a random basis. Wait for them indoors if possible. Specify the route you want the taxi to follow.

- In renting a vehicle, select a plain car, minimize the "rich American look". Consider not using a government vehicle that announces its occupants status.

- Safeguard vehicle keys.

- Pay attention to vehicle maintenance. Correct any noted problems that could cause the vehicle to stall. Ensure tires have sufficient tread.

- Keep gas tank at least 1/2 full at all times.

- Prior to getting into the vehicle, check beneath it, looking for wires, tape or anything unusual. Look for scuffs on pavement that could indicate someone was underneath the vehicle. Display the same wariness before exiting your vehicle.

- Avoid late night travel. Avoid known danger areas, isolated roads and dark alleys.

- If you have a driver, develop a simple signal to be used in case of trouble.

- Travel with companions or in a convoy when possible.

- Check the reliability of permanently assigned drivers.

- Attend special defensive driving training if available.

- When parking vehicles, secure car doors and lock garage doors.

- Habitually ride with seat belts buckled, doors locked, and windows closed.

- Do not allow your vehicle to be boxed in. Keep a minimum of eight feet between your vehicle and the one in front of you.

- Be alert for surveillance or danger while driving or riding.

- Know how to react if surveillance is suspected or confirmed. Do not stop or do anything to confront suspected surveillance. If possible, get a description of the car and its occupants. Drive to the closest safe haven and report it immediately to appropriate security officials.

- If your vehicle is under attack, attempt the following: Without subjecting yourself, passengers, or pedestrians to harm, try to draw public attention to your car (flash lights, sound horn, etc.). Put another vehicle between you and your pursuer. Execute an immediate turn and get out of the attack zone. If the road is blocked by terrorists vehicles…don't stop! Ram the blocking vehicle if necessary. Hit near rear fender of blocking vehicle at full power and drive through. Don't take your foot from the accelerator. Go to the closest safe haven and report the incident immediately to appropriate security officials.

- Do not stop to assist another vehicle, which appears to be broken down. Call and report it to the local authorities.

HOSTAGE SURVIVAL

The totally unpredictable nature of terrorism makes it impossible to be 100% secure. The possibility always exists, no matter how slight, you or members of your family will become victims of a terrorist incident regardless of how many precautions you take or how diligently they are followed. The following suggestions and guidelines have been obtained from people who have survived terrorist hostage or kidnapping situations and have witnessed the murders of those who have not survived.

- Stay calm and have faith; maintain your dignity and self-respect. Do not display bravado or cowardice.

- Stay alert for possibilities for escape. Ensure the odds of success are in your favor or do not attempt it.

- Be certain you can explain everything on your person.

- Do not criticize or antagonize your captors.

- Be prepared to be accused of being a member of the Central Intelligence Agency (CIA) or other intelligence organization.

- Make a mental note of everything that goes on - sounds, descriptions, times, phone numbers, etc. Leave evidence at all locations you are taken to assist police in their search. Do this only if it will not endanger you.

- Anticipate isolation and other methods to break or disorient you.

- Attempt to locate yourself as far away from your captors as possible. Should police attempt a rescue, you will be out of the line of fire.

- Set up a schedule of mental and physical activity and follow it.

- Comply with all instructions as well as you can.

- Don't be afraid to ask (don't demand) for anything (e.g., books, paper, medical attention, etc.)

- Eat whatever they give you and do not refuse any favors.

- Beware of a possible unconscious shift in your loyalties to your captors.

- The likelihood of becoming a hostage is slim; however, you must be prepared to survive the ordeal should it happen. An important point to remember is that the longer you are held, the greater your chance of surviving.

ASSISTANCE ABROAD

U.S. Consular officers are located at U.S. Embassies and Consulates in most countries abroad. Consular officers can advise you of any adverse conditions in the places you are visiting and can help you in emergencies. If you plan more than a short stay in one place, it is advisable to register with the nearest U.S. Embassy or Consulate. This will make it easier should someone at home need to urgently locate you or in the unlikely event that you need to be evacuated due to an emergency. It will also facilitate the issuance of a new passport should yours be lost or stolen. Should you find yourself in any legal difficulty, contact a consular officer immediately. Consular officers cannot serve as attorneys or give legal advice but they can provide lists of local attorneys and help you find legal representation. Consular officers cannot get you out of jail. However, if you are arrested, ask permission to notify a consular officer - it may be your right. American consular officers will visit you, advise you of your rights under local laws, ensure that you aren't held under inhumane conditions, and contact your family and friends if you desire. They can transfer money, and will try to get relief for you, including food and clothing in countries where this is a problem.

A FINAL WORD

Now that you are aware of the basic precautions which should be taken during your trip, take some time to put all of this information into perspective. We have fulfilled our requirement to brief you. If you follow these precautions and use your own good common sense, you will reduce the risk of encountering problems; but remember, carefulness need not become an obsession. **This is YOUR trip. Enjoy it**!

EXHIBIT 3-5

COUNTER ESPIONAGE (CE) AWARENESS BRIEFING

You must have a hundred things on your mind before your trip abroad, but I'm going to add to your mental baggage today with some serious thoughts on a serious subject. The foreign intelligence threat to U.S. military and civilian personnel continues despite the end of the Cold War. Personnel are now, more than ever, communicating with foreign nationals from all over the world. Foreign intelligence services make it their business to learn the identities

of Americans. Their main objectives are to induce Americans to either willingly or unwillingly reveal U.S. defense, security, law enforcement, industrial, scientific and technical information and/or to recruit them, through compromise and black-mail, to collect information for them upon their return to the U.S.

Traveling to or through foreign countries, you will be in a position for possible exploitation attempts - because you are an American who has access to classified information, because you will be operating on unfamiliar ground, and because you probably aren't convinced that YOU could ever be of interest to foreign intelligence. Well, chances are you haven't ever been targeted by a foreign intelligence service, but they are always on watch for any American who may cooperate with them. I certainly don't intend to frighten you, or dissuade you in any way from your journey, but you have to be doubly careful that you don't place yourself in jeopardy.

- Visa applications are routinely scrutinized by intelligence services to determine your immediate or future value to their intelligence operations. In order to avoid possible difficulties in this area, it is important that you fill out the forms truth-fully and accurately. It is especially important that you name any relatives that you intend to visit in the host country.

- When obtaining visas, travelers should ask the appropriate consular office how much foreign currency (U.S. and other) and what valuables may be taken in and out of the countries to be visited. You may not be allowed to import local currency into the country you are visiting. Make sure you have enough money for the trip, and strictly follow the approved itinerary. Never exchange money with strangers on the street.

- You may wish to carry gifts for friends or relatives with you. Items to be carried as gifts should be neither controversial nor prohibited. Do not bring pornography, narcotics or political material. pornography laws of many countries are far stricter than those in the U.S., and you should avoid taking any magazines or other materials that might be considered pornographic. Any over-the-counter or prescription drugs should be in a clearly marked container and in reasonable quantities to convince authorities that they are for your personal consumption.

- Do not carry with you (on behalf of a third party) any letters, messages, or packages for private individuals. You may be deemed guilty of circumventing normal channels of communication, or you may be regarded as a courier for illegal or subversive purposes.

- It is unwise for you to drive in some criteria countries. Try to use public transportation or hire a driver, as local traffic regulations may be confusing.

- Assume that your hotel room is equipped with listening or recording devices. Do not search for such devices, and do not make an issue of it if you should by chance find

one. The presence of such equipment may not be significant as it may not specifically concern you. Do not try to neutralize such devices by running tap water, playing your radio, etc. Overt efforts on your part to combat such penetration will only make you more suspicious to the intelligence services. The best defense against such devices is to avoid political or sensitive discussions. Should you discover any device of the

above kind, take no overt action against it. Continue your normal conversation, giving no indication that you have discovered it. Report it to the nearest U.S. Embassy or Consulate and to your Command Security Officer (CSO) during the Counter Espionage (CE) Awareness Debriefing (upon your return).

- Beyond your hotel room, you should assume that conversations in vehicles, train compartments, restaurants, conference rooms and other public places may be monitored. It is technically possible to monitor your conversations in open, outdoor areas; however, those areas are normally more secure than indoor locations.

- Avoid unnecessary discussions concerning your job, your work place and other official matters. Also avoid discussing other U.S. employee's habits, character or other matters which reveal weaknesses or idiosyncrasies.

- Assume that your personal luggage will be searched at some time in your hotel room. If you discover evidence of this, do not make a big issue of it. Positive evidence of such activity, however, should be reported to the nearest U.S. Embassy or Consulate and to your CSO during the CE debriefing. It is just as well not to bother locking your luggage, as most locks can be easily picked. If the lock cannot be picked, this will only increase the curiosity of the intelligence agent and the lock may be broken. Never leave your luggage unattended if it contains valuable papers or documents you do not wish anyone else to read. If you surprise someone searching your possessions, don't take any violent or physical action, but report the incident to appropriate security officials.

- You may receive a wrong number or otherwise mysterious telephone call in your hotel room at any hour of the day or night. Don't let this unduly upset you. It may be a crude but effective method of determining whether or not you are in your room, or it may be only a result of poor telephone service.

- Be particularly cautious in your relations with guides, interpreters, and travel agency personnel as these people are often used by intelligence services.

- You may be placed under physical surveillance as you travel either on foot or by vehicle. You may suspect you are being observed when actually you are not. In either event, the best tactic is to ignore it. intelligence agents observe visitors at various times on a spot-check basis for no apparent reason. On the other hand, they may be collecting detailed data concerning your activities in preparation for a more direct intelligence approach. Do not attempt to lose the surveillance. If you are actually being followed for intelligence objectives, you will be covered by a team of several agents and your evasion attempts will only make you more suspicious. -You probably will be allowed to take photographs with your personal camera, but be careful not to photograph restricted areas. You should refrain from taking photographs of aircraft, military and police installations or personnel, industrial

structures, harbor, rail and airport facilities and border areas. Some countries also resent your photographing items which put them in a bad light such as slum areas, public drunks, scenes of civil disorder or public disturbances. If you do take such photographs your film (and camera) may be confiscated.

- Be particularly cautious in approaches which may be made offering social companionship, especially of a sexual nature. Many of these persons are plants of intelligence services and will offer themselves to you for the purpose of getting you in a compromising situation which will be followed by a blackmail threat to force your cooperation in intelligence activities. Under no circumstance should you seek or accept this kind of social companionship in a criteria country. The intelligence services are fully aware of the possibilities inherent in human frailties, and will capitalize immediately upon any indication of immoral or indiscreet behavior of American travelers. Even when failing to detect a vulnerability, agents have attempted entrapment of innocent travelers. For this reason, you should maintain the highest level of personal behavior at all times. Avoid long walks at night alone and always try to be in the company of someone you can trust. Be especially careful to stay well within your capacity for alcohol so as not to weaken your defenses, lose your self-control or impair your judgment.

- Do not accept from anyone (including friends, relatives or professional contacts) letters, photographs, packages or any other material to be smuggled out of the country or carried in your effects when you depart. Be firm in your denials in these matters as such requests may be acts of intelligence provocation to entrap you.

- Bear in mind that there are many political, cultural and legal differences between the U.S. and foreign countries. Actions which are innocent or, at worst, carry wrist slapping penalties in the U.S., are often considered serious offenses against the law in other societies. Persons violating the law, even unknowingly, run the risk of arrest or expulsion. Do not, for instance, take souvenirs from hotels or institutions however insignificant in value they may appear.

- Do not engage in any private currency transactions with individual citizens. Do not try to sell or trade any personal items such as clothing which you have brought into the country or purchase bargains from street peddlers or other questionable vendors.

- Do not engage in black-market activities. Many countries have laws governing exportation of art work and historic relics. Be familiar with these laws if you intend to purchase such items and make these purchases only at official establishments.

- Should you be detained or arrested for any reason by police or other officials of these countries, be cooperative but insist promptly, politely and repeatedly if necessary, that the U.S. Embassy or Consulate be notified. Do not make any statements or sign any documents you do not fully understand until you have had an opportunity to confer with an embassy representative. You may possibly be accused of having some connection with an American intelligence service or of having accepted an assignment by such service to be carried out in the host country. You should make no

admission whatsoever indicating you have ever had any dealings under any circumstances with any U.S. intelligence agency.

- Mail which you receive or transmit may be subject to censorship. In all mail you write prior to, during, or after your visit, make no reference to classified information or reveal information of possible value to a foreign intelligence service. Be careful when

  writing to or about relatives or friends in these countries as they may become targets for investigation or exploitation.

- Immediately report to the U.S. Embassy or Consulate and your CSO (during the CE debriefing) any attempts by representatives of foreign countries to:

❖ Establish a personal or professional relationship.

❖ Obtain information through monetary payments, bribery, observation, collection of documents, or by personal contact.

❖ Coerce personnel by blackmail, threats against or promises of assistance to relatives living under their control.

❖ Exploit discontented personnel or those with personal
❖ difficulties.

❖ Intimidate, harass, entrap, discredit, search, spy on, or recruit personnel.

❖ Induce personnel to defect or induce those who have fled from another country to re-defect.

Above are some of the pitfalls that may POSSIBLY befall an American traveler. If you respect local laws and customs, are honest in your dealings and behave discreetly, you PROBABLY will not be entrapped by a foreign intelligence service and you PROBABLY will not have any problems. Have a good trip and come home safely.

EXHIBIT 3-6

COUNTER ESPIONAGE (CE) AWARENESS DEBRIEFING

Now that you have returned from your trip to a criteria country (or a meeting), it is necessary that you be debriefed. You now have the opportunity to report any incident, no matter how insignificant it may have seemed. Specifically, we are interested in any actions by representatives of criteria countries that attempted to:

- Establish a personal or professional relationship.

- Obtain information through monetary payments, bribery, observation, collection of documents, or by personal contact.

- Coerce personnel by blackmail, threats against or promises of assistance to relatives living under their control.

- Exploit discontented personnel or those with personal difficulties.

- Intimidate, harass, entrap, discredit, search, spy on, or recruit personnel.

- Induce personnel to defect or induce those who have fled from another country to re-defect.

- The following are a few questions that may help you remember:

- Did anyone attempt to ask questions about your place and nature of your employment, background, hobbies, cultural and sports interests, travel desires, or other personal preferences?

- Did you receive any invitations to dinner, cocktail parties or recreational activities?

- Did anyone attempt to offer you social or sexual companionship?

- Did anyone attempt to offer to assist you in obtaining visas, export permits, licenses, etc.?

- Did anyone attempt to give you letters, packages, etc. to be delivered to someone else?

- Was there any evidence that you may have been followed?

- Did you find any evidence of listening or recording devices in your hotel room?

- Did you find any evidence of your luggage or hotel room being searched?

- Did any suspicious persons telephone you or knock on your door?

- Can you think of anything else that may be important?

If you answered yes to any of these questions, you will be required to provide a detailed narrative of the incident to G-CFI via your cognizant SECMGR. Appropriately trained security personnel will take it from there.

Foreign intelligence services pose a very serious threat to our national security. It is through your understanding and accepting your responsibility to report such incidents that we, together, can thwart potential foreign intelligence efforts.

EXHIBIT 3-7

TRANSFER BRIEFING

Now that you are transferring, you are no longer authorized access to classified information at this unit. ALL classified material in your custody must be returned at this time.

Your security clearance has been administratively withdrawn without prejudice. If access is required at your next unit, your eligibility will be reviewed and a clearance will be requested

as necessary. (NOTE: At this time, explain the individual's current clearance eligibility and what they need to maintain or upgrade that eligibility).

You must never divulge classified information, orally or in writing, to any unauthorized person or agency.

You must promptly report to CSO, Cognizant SECMGR or the nearest Coast Guard unit, any attempt by an unauthorized person to solicit classified information from you during your transfer period.

You remain subject to the espionage laws and criminal codes applicable to the unauthorized disclosure of classified information, as explained in the Classified Information Nondisclosure Agreement (SF 312), which you signed when you were granted access.

NOTE: Attached is an optional Security Outbrief Questionnaire that may be given to the individual to voice their opinions and concerns regarding security. The questionnaire should be retained by security personnel to aid in identifying and evaluating strengths and weaknesses in the Coast Guard Security Program.

SECURITY OUTBRIEF QUESTIONNAIRE

1. What was the single-most security hazard you observed at this unit? (e.g., personnel taking classified material home to work on, unauthorized people in spaces, misuse or theft of government property, etc.)

_____
_____
_____
_____

2. How would you fix the problem? _____
_____
_____
_____

3. Did you receive security training when you first reported here?
Yes _____ No _____ How long ago?_____

4. Did you receive periodic security training?
Yes _____ No _____ About how often?_____

5. Was the training worth your time? Yes _____ No _____

6. If training was not adequate, what should be improved? _____
_____
_____

7. On a scale of 1 (the lowest) to 10 (the highest), how would you rate the security awareness and practices of your co-workers?_____
_____
_____

8. What are the major strengths of the Coast Guard Security Program? _____
_____
_____

9. What are the major weaknesses of the Coast Guard Security Program?
_____
_____

10. Any other comments or suggestions? _____
_____
_____
_____

THANKS FOR TAKING THE TIME TO COMPLETE THIS SURVEY!

EXHIBIT 3-8

FINAL TERMINATION BRIEFING

Now that you are no longer authorized access to classified information, we need to discuss your future security responsibilities. But first, ALL classified material in your custody must be returned at this time.

Termination of your access to classified information now does not terminate your future responsibility to protect that classified information to which you have had access. You must never divulge classified information, orally or in writing, to any unauthorized person or agency. If you ever prepare a lecture, write an article, etc., that you believe contains classified information, you are encouraged to submit the material for review to Commandant (G-CFI).

You must promptly report to the Coast Guard Office of Security Policy and Management (G-CFI) via your cognizant Area/District Security Manager any attempt by an unauthorized person to solicit classified information from you.

You remain subject to the espionage laws and criminal codes applicable to the unauthorized disclosure of classified information, as explained in the Classified Information Nondisclosure Agreement (SF 312), which you signed when you were granted access.

When you have completed this briefing, you will be asked to sign the Personnel Security Record (CC 5274) (for military) or the Security Termination Statement (DOT 1600.10) (for civilians). Read them. By signing these statements, you verify that you have received a briefing; returned all classified material in your possession; and you understand your future security responsibilities under the law.

EXHIBIT 3-1

SECURITY BRIEFINGS REQUIREMENT SCHEDULE

BRIEFING	AUDIENCE	SUBJECTS	FREQUENCY
Arrival	New employees	Security points of contact, internal security procedures, identification and protection of classified material, loss/crime prevention responsibilities, OPSEC	Upon arrival, as occurring
Access	Employees granted access to classified information	Clearance and eligibility, classified material handling (storage, marking, transmission, destruction, etc.), attempts to solicit, reporting violations/compromises, non-disclosure agreement	Prior to granting access as occurring
Refresher	All employees	Changes in security policies or procedures, specific problem areas, loss /crime prevention, OPSEC, counterintelligence reminders, etc.	Annually
Coast Guard AT/FP Level I	Employees traveling to a foreign country	Hotel/vehicle/airline security, personal safety, travel advisory hotline, terrorism awareness	Annually
Counter Espionage Awareness	Cleared employees traveling to or through a criteria country (or attending a meeting)	Foreign intelligence exploitation, attempts to solicit, contacts, approach techniques, security precautions, personal safety	As required